Hacking Passports

Exposing the Vulnerabilities of 'Smart Card' Technology

BY ROB SANCHEZ

If there is one document that serves as a ticket to just about anywhere in the world it's the United States passport. Passports are the ultimate breeder documents for almost everything that requires identification. Owning one is essential for millions of international travelers, and in many countries they are used for identification and transactions. Security of the personal information on passports is critical for ensuring privacy, and yet the expediency and cost savings realized by offshore outsourcing have been a more important priority than using common sense measures to reduce the risks of hacker attacks.

In order to thwart fraud, identification theft, and counterfeiting, the U.S. government and most other nations in the world embarked on programs to design a new generation of passports with "smart card" technology. Despite the grandiose efforts to incorporate technology into the passports, about all that has been accomplished is to shift the tools of crime from color copy machines to computers.

Smart technology gives the public a false sense of security because of its high-tech mystique. Smart technology, like any electronic device, is vulnerable to tampering. Software code and the microelectronics used to make the passports are vulnerable to attack, and the risk is heightened by outsourcing the engineering and production of the components to private companies that are foreign owned and located overseas. Some of the nations involved are hostile to the United States, or they don't have the law enforcement infrastructure to control criminals.

A recent *Scientific American* article about hardware hacking provides excellent background for the problems with smart technology. The article didn't explicitly mention passports, but the same issues apply.

As if software viruses weren't bad enough, the microchips that power every aspect of our digital world are vulnerable to tampering in the factory. The consequences could be dire:

• Integrated circuits are increasingly complex and capable — but also increasingly vulnerable to attack.

• The circuits typically include designs from many sources. A "Trojan" attack hidden in one of these designs could surface long after the circuit has left the factory.

This is one possible way that we might experience a large-scale hardware attack — one that is rooted in the increasingly sophisticated integrated circuits that serve as the brains of many of the devices we rely on every day. These circuits have become so complex that no single set of engineers can understand every piece of their design; instead teams of engineers on far-flung continents design parts of the chip, and it all comes together for the first time when the chip is printed onto silicon. The circuitry is so complex that exhaustive testing is impossible. Any bug placed in the chip's code will go unnoticed until it is activated by some sort of trigger, such as a specific date and time — like the Trojan horse, it initiates its attack after it is safely inside the guts of the hardware.

"The Hacker in Your Hardware: The Next Security Threat," by John Villasenor, *Scientific American*, August 4, 2010 [1]

Tampering with passport hardware is not difficult when the engineers who designed it or the factory workers that assembled it are the saboteurs. Detection and prevention of covert sabotage is much more difficult when the production process takes place in dispersed locations worldwide where the U.S. government has little influence.

***Rob Sanchez** keeps track of non-immigrant visa and offshoring developments at his website, www.jobdestruction.info. He also publishes the* Job Destruction Newsletter. *To get on the free mailing list, send an e-mail to: news@JobDestruction.info*

Each e-passport contains a microprocessor chip and a memory that stores the software for the operating system. Software is implanted into a small computer memory chip in much the same way as the BIOS is programmed on a home computer. It's at this stage that hacking is the easiest to accomplish by technically proficient infiltrators who could slip a small piece of code into the software that is, for all practical purposes, invisible. The code could be programmed as a Trojan horse that is only activated when the passport is queried with a surreptitious request. Trojans that have been put into code at this level would be virtually impossible to detect.

The U.S. Government Accountability Office (GAO) recognizes that malicious code could be slipped into the passport hardware. It's worth noting that they give the public no more than a vague "reasonable assurance" that the passports are secure:

> If properly validated, the digital signatures on State's e-passports should provide those reading the chip data, including DHS [Department of Homeland Security], reasonable assurance that the data stored on the chip were written by State and have not been altered. Proper validation includes verifying that the document signer certificate was issued by the State Department.
>
> *Border Security*: Better Usage of Electronic Passport Security Features Could Improve Fraud Detection, GAO, January 2010.[3]

The components for the e-passport are manufactured in locations all over the globe in places such as Asia and Europe. Brian Ross of ABC News did an excellent report investigating how outsourcing to foreign countries exacerbates security problems: "Operation Outsourced: Security of U.S. Passports" can still be watched online. [2]

ABC made the connection that critical parts of the passport are made in Thailand — a country with a significant radical Islamic population. What ABC didn't make very clear is that Thailand is just one of dozens of nations that are involved in the manufacture of passports.

The following statement by the GAO describes the globalized design and manufacturing of passports. It is alarming to read because the product supply and design chain is so similar to the scenarios described by the *Scientific American* article.

> In producing e-passport booklets for State, the Government Printing Office (GPO) has tapped into the existing global smart card industry, resulting in a wide number of different companies involved in the e-passport chip production and inlay process. Two separate companies were awarded contracts to supply chips for the U.S. e-passports. Infineon, a German company, fabricates its own chips and embeds a commercial operating system from a third-party company on them. Gemalto, a Dutch company, obtains chips from NXP, a Dutch semiconductor manufacturer. Gemalto provides NXP with its own operating system, which NXP embeds within the chip prior to shipping the chip to Gemalto.
>
> Better Usage of Electronic Passport Security Features Could Improve Fraud Detection, GAO, January 2010 [3]

The manufacturing trail for passports is complex because it is dispersed over many different countries and companies. Identities of most of the companies who are suppliers are withheld by the GPO for security reasons, but they name a few of the major ones. The NXP website [4] for the Dutch-owned company claims to have 13 manufacturing sites worldwide and 26 R&D centers located in 12 countries. NXP engineers in foreign countries designed the software to control the smart chips, so it's doubtful that our government knows who designed it or where. Gemalto is a company jointly owned by the Dutch and French with locations worldwide. Infineon [5] is a German company that makes passport hardware for many different countries including China and the U.S.

> The Chinese government is using security microcontrollers of Infineon Technologies AG (FSE: IFX / OTCQX: IFNNY) for its new electronic passports. Infineon today announced that it recently started deliveries to the Chinese electronic passport project which volume-wise is one of the world's two biggest electronic passport projects. As of the first quarter of 2010, all new Chinese passports will be issued as electronic passports. The Chinese government estimates that, beginning in the first full year of the roll-out, about 6.5 million electronic passports will be handed out annually to citizens, diplomats and government workers. In total, there are currently more than 30 million passports in circulation in China, which are usually valid for ten years. China Selects Infineon's Security Chips for

> Electronic Passports, Infineon Press Release, November 11, 2009 [6]

Sharing common technology platforms with other countries is risky because hackers worldwide can concentrate their efforts on fewer systems to break into. As these technologies proliferate, there will be increasing probabilities that somebody will figure out how to hack them, and the motivation to do so will increase as the value of the information expands. Sharing those systems with enemies such as China or with countries that have large terrorist organizations exacerbates the risk. One only has to look at the worldwide popularity of the Microsoft Windows operating system to see a common example that demonstrates how a popular platform encourages the proliferation of malicious viruses.

China's desire for hacking passports cannot be underestimated. In 2007 Smartrac filed a complaint in the International Court of Justice based in The Hague. Smartrac accused China of stealing their patented technology for e-passport chips. It must now be assumed that China has obtained the secrets of the technology, so their engineers have figured out all the vulnerabilities of e-passports.

Passports are supposed to be valid for 10 years, so that's how long the Chinese and the world's best hackers have to compromise them. Just imagine how simple it would be if a hacker with today's powerful computers was tasked with hacking a 10-year-old computer!

E-passports are so globalized it's fair to assume that all citizens from all nations are in jeopardy of privacy breaches. If personal information is pried out of passports, it will not matter to the victims if the system is upgraded or improved because biometric information such as fingerprints, face pictures, and eye scans lasts the duration of a lifetime, not a decade.

Worldwide, nations are trending towards standard designs and common databases for passports. As this trend progresses, governments will want to simplify data sharing by making a worldwide database of everyone in the world. Databases will either be centralized or the data of individual nations will be linked together by networks.

The development of a worldwide database almost seems inevitable. Policy decisions concerning passports are mostly invisible to the public as they are made and implemented by faceless bureaucrats instead of elected officials that are accountable to the people of the U.S. Most of the decisions on passport standards and policies aren't even made in the U.S.— they are made by international committees and agencies such as the International Civil Aviation Organization (ICAO), a specialized agency within the United Nations, and the International Organization for Standardization (ISO), based in Geneva.

Passports are morphing into global identification cards, and the American public has almost no voice or control in the way they are to be manufactured or used. It wouldn't be much of a stretch to say that the U.S. has almost no control over e-passports. Even U.S. law is out of control, considering that the Visa Entry Reform Act of 2002 doesn't require the U.S. government to make a radio frequency identification device (RFID) passport and it doesn't give the State Department or the GPO the statutory authority to manage one.

Globalized systems have inherent security problems because they are connected to networked computers that affect large groups of people simultaneously. The story about a recent malfunction of a European smart card system received very little media coverage in the U.S., but it should have because it serves as a warning about what the future holds:

> "Late Millennium bug" hits Germany leading to over 30 million debit and credit cards damaged and incapable of transactions. The mishap was reported to have occurred as a result of a programming failure, which left the German credit and automated teller machine (ATM) cards unable to deal with the change in year from 2009 to 2010.
>
> The bug has left cardholders unable to use their payment cards in drawing cash from the cash machines or make payments throughout Germany and abroad.
>
> Gemalto Counts Cost of New Year Bug, *Smart Card News*, January 2010 [7]

Robert Mocny, acting director of the Department of Homeland Security US-VISIT program, described the push for globalized identification in a speech at an international biometrics and ethics conference in 2006. US-VISIT is a system that screens foreigners for criminal or terrorist connections using their biographical and biometric data. While describing why countries have an obligation to share the personal information of travelers with other nations, Mocny admitted [27] to the desire to implement a worldwide system when he said, "We have an ethical responsibility to make the vision of a global security envelope possible sooner rather than later."

Citizens of the U.S. have no choice whether their passports have the e-passport technology because all passports issued since 2007 are required to include it. E-passports can be identified by the international logo

on the front cover.
http://hasbrouck.org/images/rfid_logo_position.jpg

According to the State Department, [8] over 48 million U.S. passports have been issued with e-passport smart technology per fiscal year. Worldwide over 100 million e-passports are in use by about 50 different countries.

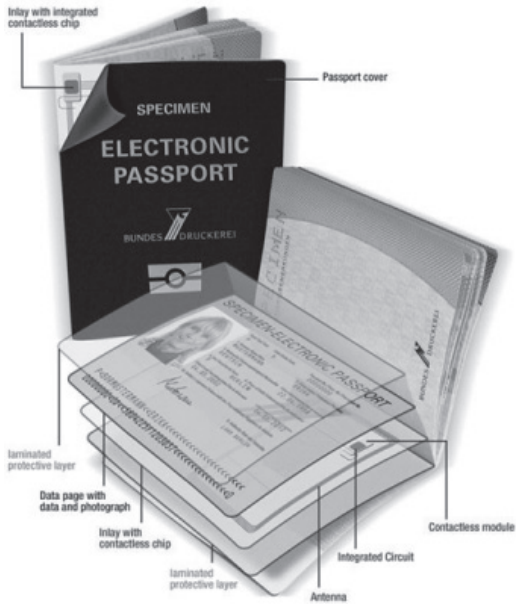
U.S. e-passports per fiscal year

2009 - 13,486,085
2008 - 16,208,003
2007 - 18,382,798

Total - 48,076,886

As of June 2010, the GPO claimed that they have delivered more than 55 million [8] blank e-passports without a single security breach. Boasting over their security success rate is somewhat of an empty claim because the e-passport system is only partially completed. Most U.S. passports are used in the conventional fashion as a paper document because the DHS is behind on installing passport scanners and the networked computers necessary to make the system fully operational. Responsibility for installing scanners was pushed onto the Customs and Border Patrol (CBP), but that hasn't helped to speed things up. As of January 2006 only 500 scanners have been deployed, and since then due to lack of funding no additional ones have been installed. If the CBP decides to buy more scanners, they will most likely purchase ones that are made overseas so even those devices are suspect.

So, let's review the entire picture: The brain of the passport is a smart chip that is manufactured somewhere in the world by NXP, Infineon, and probably contracted fabrication plants. The smart chip and associated hardware are shipped to Gemalto for packaging and programming. Integration of the components is completed after they are shipped to Smartrac in Minnesota or Thailand for assembling the inlay. The inlay is a laminate containing an RFID and antenna. Outer layers of sheet material, such as the passport cover stock, security paper, or laser-engravable polycarbonate, protect the electronics on the front of the passport.
http://infosecurity.us/images/rfid_passport.jpg



The GPO is the sole provider of blank U.S. passports, but they are merely the front end of a very large and complicated process. Blank passports are sold exclusively by the GPO to the Department of State. The State Department has a procedure called "personalization" when the personal information of the passport owner is implanted into the smart card. The easiest way to counterfeit passports is to steal blank passports at this stage of the operation because they could be implanted with fake biometric data that could be used to confound security databases.

The final product is shipped to the U.S. Government Printing Office (GPO) to employees at secure production facilities in Washington, D.C., and at the Stennis Space Center in Mississippi [9]. It's at those locations where somebody puts a stamp on the document that says "Made in the USA." The GPO shipped the blank passports to the State Department by unsecured FedEx until they decided to use an armored car company. There was a debate about whether to contract the armored car out to a foreign-owned company, but a few diplomats at the State Department raised loud enough objections to stop that from happening.

Does the entire process sound confusing? That's because it is! There are plenty of reasons to doubt that government bureaucracies are capable of keeping track of the interconnected manufacturing process. At least 60 suppliers all over the world are used to manufacture components. Government agents inspect the supply chain, but there are only about 30 agents that travel all over the world to inspect the suppliers. Inadequate manpower problems of this type are almost a guarantee that security gaps will occur. Typically inspectors target about 16 companies that are considered to be the most critical. During an audit in 2006, most of those companies didn't have documented security plans — and adding to the concern, due to budget cuts the GPO only has one employee to oversee the formal security supply chain assessment process. [10]

This statement by the GPO isn't very reassuring:

> The sites are spread across several countries, and within some countries there may be multiple sites. For example, for both Infineon and Gemalto, production of the chips involves several sites within Europe. [3]

The GAO explains the globalized passport design and manufacturing system in more detail:

> In producing e-passport booklets for State, GPO has tapped into the existing global smart card industry, resulting in a wide number of different companies involved in the e-passport chip production and inlay process. Two separate companies were awarded contracts to supply chips for the U.S. e-passports. Infineon, a German company, fabricates its own chips and embeds a commercial operating system from a third-party company on them. Gemalto, a Dutch company, obtains chips from NXP, a Dutch semiconductor manufacturer. Gemalto provides NXP with its own operating system, which NXP embeds within the chip prior to shipping the chip to Gemalto. [3]

The types of cyber attacks on passports are as vast as the imagination of criminals and terrorists. The Center for Public Integrity (CPI) gave this warning in June, 2010:

> Thai workers there assemble inlays that embed wireless transmitters and sophisticated computer chips that store biometric and other personal information used by customs officials and border guards to verify the identities of those who enter the United States.
>
> The U.S. Government Printing Office, the agency charged with producing the new e-Passports, has been warned repeatedly since 2006 by its own security officer that the Thai manufacturing site posed a "potential long term risk to the USG (U.S. government's) interests," according to inspection reports obtained by the Center for Public Integrity and ABC News.
>
> U.S. Lacks Basic Security for e-Passport Manufacturing, Key Tool for Border Security Made in High-Risk Locations, by John Solomon, June 14, 2010 [23]

More recently the CPI published another article, and things don't look any better:

> A decade after the Sept. 11, 2001, terror attacks brought to light the dangers of fake IDs, federal undercover agents are still able to easily obtain genuine U.S. e-Passports using clearly fraudulent information that should have raised red flags at the State Department.
>
> Undercover Feds Able to Easily Obtain Fraudulent e-Passports, by John Solomon, July 29, 2010 [24]

Although most U.S. passports that are in use haven't been used as e-passports due to the lack of installed scanners, they still pose a security risk for anyone that carries one because they could transmit personal information. Passports use RFID technology, which means that they could in theory broadcast personal information to surveillance by hackers who shouldn't have access by a process called skimming, which often involves nothing more than a laptop computer that is configured as a scanning device.

E-passports are supplied with a shielding envelope that attenuates all but the most sophisticated attacks using advanced receiver and antenna equipment. Owners have to make sure that their passport is completely closed for the shield to be effective. Keeping passports closed at all times is problematic and not as easy to do in Europe where passports are used for various forms of identification for credit cards, to lease cars, or to register to vote, etc. The following excerpt from *eWeek* explains the problems with RFID:

> At the same time, there have been persistent outcries from privacy and security advocates regarding the use of Radio-frequency identification (RFID) technology in passports in order to transmit and receive data from scanners. It's not that difficult to imagine some

> rogue code inserted into the smart chip that would only broadcast information when it received a specific code from a spy, terrorist, or criminal. The hack could be programmed to respond when a specific query is transmitted to the RFID but it will operate normally in all other situations. Information transfer would be almost impossible to detect because it could happen in a fraction of a second at any place somebody might be carrying a passport. Just imagine if an enemy government used it to track our spies!
>
> In response, the State Department has increased the security technology for the electronic passports, adding both shielding and access control measures.
>
> Infineon Announces Deal for U.S. Passport RFID Chips, Renee Boucher Ferguson, *eWeek*, 2006-08-29 [12]

Hardware hacks to obtain personal information are a very real threat to privacy because worldwide governments are embedding biometric information on passports. [11] To get an idea what types of information could be stored, one only needs to look at the European Union, [13] which established a biometric standard that requires a face picture and fingerprints. In the U.S. the RealID Act would require similar biometric information. So, just imagine the ramifications if an unsuspecting victim lost his or her biometric information to a criminal hacker: faces and fingerprints can't be changed (barring plastic surgery or amputation), so exposing these data could affect innocent victims for their entire lifespan.

Privacy in RFID Tags

Some immigration reform groups support the RealID Act. They tend to ignore the privacy concerns because they think this technology will make it nearly impossible to be in the U.S. illegally. Their enthusiasm for national identification cards is misplaced. They are probably not aware of the real security issues involved, as outlined in this article. Few realize how easy it is to clone them to assume fake identities.

Hacking smart chips and the RFID interface aren't the only things to worry about, although that is one of the scariest scenarios because attacks of that kind would be virtually impossible to detect until the data are compromised. Two excerpts below describe examples of successful hacker attacks:

> A security expert has cracked one of the U.K.'s new biometric passports, embarrassing the British government which has touted [them] as a way of cutting down cross-border crime and illegal immigration.
>
> The attack, which uses a common RFID reader and customised code, siphoned data off an RFID chip from a passport in a sealed envelope, said Adam Laurie, a security consultant who has worked with RFID and Bluetooth technology. The attack would be invisible to victims, he said.
>
> "That's the really scary thing," said Laurie, whose work was detailed in the Sunday edition of the Daily Mail newspaper. "There's no evidence of tampering. They're not going to report something has happened because they don't know."
>
> UK biometric passports succumb to hack, by Jeremy Kirk, IDG News Service, March 6, 2007. [14]

Recently a group of Indian hackers were caught hacking system software:

> Seven people were arrested in Andhra Pradesh for hacking the online passport application software of the Hyderabad regional passport office, police said Friday. Police Commissioner A.K. Khan told reporters that seven people, among them five passport agents, were arrested and a search was on for two other agents involved in the racket.
>
> Seven held in Andhra for hacking passport software, *Thaindian News*, June 4, 2010 [15]

The U.S. government recognizes the security threat that outsourcing to Thailand poses. In June of 2010, Steve LeBlanc, Managing Director, Security & Intelligent Documents, GPO, announced that the assembly of the passports will move to Chanhassen, Minnesota. [16] Shifting the assembly plant operations of the Dutch-

owned company Smartrac from Thailand to Minnesota was a good idea to improve security, but the move is no panacea. Changing locations is somewhat futile since Smartrac will still produce passport inlays by using the same complicated chain of foreign suppliers for the components. The threat of compromised hardware is unlikely to improve much because by the time Smartrac gets the parts to assemble the inlay, the malicious code would already be in place. Smartrac would be very unlikely to discover the sabotage in the assembly process.

Smartrac produces inlays for most of the passports in the world, so they will continue to produce inlays at their Thailand location. Smartrac could shift some of the production of inlays for U.S. passports back to Thailand if they lack capacity at the U.S. location or for any other reason they deem it necessary (like for cheap labor). As of June 2010, 20 percent of the inlays were still being made in Thailand. [17] Fraud investigators would have a daunting task if they had to do a forensic search to trace where the inlay components for a passport came from because Thailand will continue to assemble passports for other countries including the U.S. Any damage that has already been done to the system will continue until an anomaly is detected.

The most insidious and difficult to detect hacker attacks would most likely be done covertly by employees of one of the many companies that contribute to the manufacture of passports. Hiring foreign workers increases security risks because allegiance to the U.S. isn't required, and perhaps even more important, criminal background checks of foreign nationals are often difficult or impossible to do. Smartrac hires foreigners that have proof of legal residence and valid green cards or H-1B visas. Foreign nationals are allowed to work at Smartrac for various support positions, such as, for instance, "maintenance manager" and "research assistant." [18] Smartrac employs about 20 people in Chanhassen, Minnesota, which is good for the local economy although it's not clear how many of the workers are local versus foreign, and there doesn't seem to be much oversight on the criteria Smartrac uses to hire people. If foreign entities wanted to implement espionage at the Smartrac plant, the H-1B visa would be an excellent conduit for saboteurs to position themselves into the right places.

Considering that security experts within the U.S. government recognize the dangers of outsourcing the manufacture of passport components to overseas locations, why did they decide to do it? The best explanation is straight out of the mouth of the GPO when they responded to a scathing series of articles done by the *Washington Times* that raised the same question (excerpt from the *Times* followed by GPO response):

> According to interviews and documents, GPO managers rejected limiting the contracts to U.S.-made computer chip makers and instead sought suppliers from several countries, including Israel, Germany and the Netherlands.
>
> Mr. Somerset, the GPO spokesman, said foreign suppliers were picked because "no domestic company produced those parts" when the e-passport production began a few years ago. Outsourced passports netting government profits, risking national security, by Bill Gertz, *Washington Times*, March 26, 2008 [19]
>
> GPO Response:
>
> In coordination with the State Department and the U.S. intelligence community, GPO conducted a Request for Proposal (RFP), under GPO's procurement rules and regulations, to procure the required bio-metric components to build an e-passport. GPO incorporated The Buy American Act in accordance with MMAR-52-225. Those responding to the RFP all submitted Buy American Act certificates. However, many companies were able to achieve Buy American Act certification due to their North American subsidiaries. There were no U.S. companies who manufactured integrated circuits that met ICAO [ICAO is International Civil Aviation Organization] standards and/or rigorous testing. During the vendor selection process, GPO and the State Department vetted the limited number of qualified vendors through rigorous security audits. Those audits included inspections of facilities and employee background checks. GPO was shocked to learn no U.S. company manufactured an integrated circuit that met the ICAO standards and/or rigorous testing. Since 2004, GPO has encouraged U.S. companies to consider producing ICAO compliant components.
>
> GPO Responds to Second *Washington Times* Story, March 27, 2008 [20]

On first impression it may seem that the GPO is making lame excuses for buying smart chips and other components in the U.S., but the reality is that they probably couldn't find domestic suppliers no matter what

price they were willing to pay. The manufacturing sectors in the U.S. have been decimated to such an extent that foreign countries dominate the semiconductor business. Over the last 20 years U.S. companies have outsourced most of their production capacity offshore. *Manufacturing & Technology News* published an article that describes the trends in very stark terms: "U.S. Becomes a Bit Player in Global Semiconductor Industry: Only One New Fab Under Construction In 2009," by Richard A. McCormack, February 12, 2010. [21] Important highlights of the article:

> • In 2009, 16 fabrication plants (fabs) began construction throughout the world. One of them was in the United States.
>
> • In 2007, only 8 percent of all new semiconductor fabs under construction in the world were located in the United States.
>
> • As of 2009, the percentage of global semiconductor production capacity located in the United States was 14 percent, down from 25 percent in 2005 and 17 percent in 2007.
>
> • The United States leads the world in one category: *closures!* In 2009, 27 fabs closed worldwide, with 15 of them in the United States followed by four in Europe, four in Japan, two in China, one in Korea, and one in Southeast Asia.

According to RAND, [26] in 1980 the U.S. had about 60 percent of the world market share.

The bottom line is that it may no longer be possible for any of the electronic semiconductor components used for e-passports to be produced in the U.S. because it has lost most of its semiconductor manufacturing foundries. If the exodus of U.S. manufacturing continues it's doubtful that passports could be made in the U.S. for decades to come.

Percentage of global semiconductor capacity 2009

Japan	**25%**
Taiwan	**8%**
Korea	**17%**
U.S.	**11%**
Europe	**11%**
Middle East	**11%**
China	**9%**
SE Asia	**6%**

The lack of domestic suppliers for government-funded projects is a problem that simply wouldn't have happened before 1990 because the U.S. government considered it a national security priority to procure electronic semiconductors from domestic sources.

Several factors in the 1980s contributed to the decline of the government's ability to mandate that domestic suppliers be used for their contracts: growing consumer buying power, shrinking military budgets, and globalization. The military share of the electronics industry became insignificant compared to the civilian market by 1990 and by that time American owned companies were moving their facilities offshore as fast as they could. In some cases the military or other large buyers like NASA paid far more than commercial market prices to subsidize U.S. manufacturers so that private industry would keep fabs open, but it was a losing battle that could only stall the inevitable stampede overseas.

In view of the trend towards globalization the Department of Defense adopted a new policy called the Commercial-Off-The-Shelf (COTS) program. [22] Parts procurement by commercial producers was mandated because it was considered more cost effective to do so. National security was sacrificed in order to buy civilian components — even when they were made in foreign countries. Governmental agencies purchased from the lowest-cost suppliers even as U.S. companies were closing fabs, going out of business, and moving overseas.

Of course there is a more obvious explanation for passport outsourcing — simple greed and stupidity. In a scheme that resembles a starving man who cuts off his legs to satiate his hunger, the GPO made about $100 million in profits by selling the blank passports to the State Department. [19] More than likely, the GPO rationalizes that using domestic suppliers for components would cut profit margins from their sales to the State Department, so they use the lowest-cost bidders, who always happen to be overseas suppliers.

A video called "The Myth of Biometrics' Enhanced Security" [25] by Michael (Micha) Shafir and David J. Weiss, February 17, 2009, does an excellent job of illustrating the various threats posed by e-passports. Warning: the animated person doing the narrative is rather annoying and the video is partially an infomercial.

I spent most of my career writing embedded software and designing the related hardware at Motorola Government Electronics Division in Scottsdale, Arizona. Many of the design projects I worked on were for government secure communication applications. As a result of my professional experience I understand that these

threats are very real, even though they may sound esoteric. Hacker attacks against passports could potentially dwarf credit card and identity fraud and pose a serious threat to personal privacy and national security. ■

Endnotes

1. "The Hacker in Your Hardware: The Next Security Threat," by John Villasenor, *Scientific American*, August 4, 2010
http://www.scientificamerican.com/article.cfm?id=the-hacker-in-your-hardware

2. ABC Reports, "Operation Outsourced: Security of U.S. Passports" http://www.hulu.com/watch/157082/abc-brian-ross-investigates-fri-jun-18-2010

3. BORDER SECURITY: Better Usage of Electronic Passport Security Features Could Improve Fraud Detection, GAO, January 2010
http://www.gpo.gov/pdfs/congressional/GAO_Rpt_BorderSecurity.pdf

4. NXP Locations
http://www.nxp.com/jobs/world/index.html

5. Infineon Subsidiaries
http://www.infineon.com/cms/en/corporate/company/regional-subsidiaries/

6. *China Selects Infineon's Security Chips for Electronic Passports, Infineon Press Release,* November 11, 2009
http://www.infineon.com/cms/en/corporate/press/news/releases/2009/INFCCS200911-008.html

7. Gemalto Counts Cost of New Year Bug, *Smart Card News*, January 2010
http://www.smartcard.co.uk/members/newsletters/2010/SCN%20January%202010.pdf

8. Passport Statistics
http://travel.state.gov/passport/ppi/stats/stats_890.html

9. U.S. e-Passport facts at-a-glance, GPO
http://www.gpo.gov/pdfs/congressional/factsheet_e-passport.pdf

10. Security of GPO's e-Passport Supply Chain, March 31, 2010
http://www.gpo.gov/pdfs/ig/audits/10-06_FinRptSecGPOePassprtChain.pdf

11. ICAO: Machine Readable Passports to be Issued Worldwide by 2010, Information Handling Services, July 20, 2005
http://aero-defense.ihs.com/news/2005/icao-machine-readable-passports.htm

12. Infineon Announces Deal for U.S. Passport RFID Chips, Renee Boucher Ferguson, *eWeek*, 2006-08-29
http://www.eweek.com/c/a/Mobile-and-Wireless/Infineon-Announces-Deal-for-US-Passport-RFID-Chips/

13. Integration of biometric features in passports and travel documents
http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l14154_en.htm

14. UK biometric passports succumb to hack, by Jeremy Kirk, IDG News Service, March 6, 2007
http://news.techworld.com/security/8185/uk-biometric-passports-succumb-to-hack/

15. Seven held in Andhra for hacking passport software, *Tahindian News*, June 4, 2010
http://www.thaindian.com/newsportal/uncategorized/seven-held-in-andhra-for-hacking-passport-software-lead_100375081.html

16. GPO reassures your passport is secure, Federal News Radio, June 17, 2010
http://www.federalnewsradio.com/?sid=1982668&nid=15

17. PASSPORT SUPPLY CHAIN IS SECURE, GAO Press Release, June 15, 2010
http://www.gpo.gov/pdfs/news-media/press/10news20.pdf

18. GPO Responds to Second *Washington Times* Story, March 27, 2008
http://www.gpo.gov/pdfs/news-media/press/08news12.pdf

19. Outsourced passports netting government profits, risking national security, by Bill Gertz, March 26, 2008
http://www.washingtontimes.com/news/2008/mar/26/outsourced-passports-netting-govt-profit-56284974/

20. H-1B Visa application for Smartrac http://www.myvisajobs.com/Maintenance-Manager-Smartrac-Technology-Us-Inc.-H1B-3003062.htm

21. "U.S. Becomes a Bit Player in Global Semiconductor Industry: Only One New Fab Under Construction in 2009," by Richard A. McCormack, February 12, 2010
http://www.manufacturingnews.com/news/10/0212/semiconductors.html

22. Outsourcing Poses Unique Challenges for the U.S. Military-Electronics Community, by Randall Milanowski and Mark Maurer, *Chip Design*, 2006
http://chipdesignmag.com/display.php?articleId=752&issueId=18

23. U.S. Lacks Basic Security for e-Passport Manufacturing, Key Tool for Border Security Made in High-Risk Locations, by John Solomon, June 14, 2010
http://www.publicintegrity.org/articles/entry/2153/

24. Undercover Feds Able to Easily Obtain Fraudulent e-Passports, by John Solomon, July 29, 2010
http://www.publicintegrity.org/articles/entry/2292/

25. "The Myth of Biometrics' Enhanced Security," by Michael (Micha) Shafir and David J. Weiss, February 17, 2009
http://www.liveleak.com/view?i=8e3_1235153454

26. High-Technology Manufacturing and U.S. Competitiveness, RAND Research, March 2004
http://www.rand.org/pubs/technical_reports/2004/RAND_TR136.pdf

27. Robert Mocny statement
http://www.govexec.com/dailyfed/1106/112906tdpm1.htm