Sean Ong
COMP 116: Introduction to Computer Security
May 7, 2018

Evaluating the Security of National Electronic Identification Programs

Abstract

Since Estonia first implemented a revamped digital ID-kaart in 2002, national electronic identification (eID) programs have been gaining traction worldwide as a way for citizens to access government services efficiently and across borders. This paper evaluates the security issues of national eID programs, focusing on the first two prongs of the confidentiality, integrity, and availability (CIA) triad. It looks at three vulnerabilities affecting eID systems, including two specific cryptographic flaws — Coppersmith's attack and Return of Coppersmith's Attack (ROCA) — and a more general weakness in our current reliance on certification as a proxy for security.

Introduction

National electronic identification (eID) programs have risen to mainstream prominence: As of early 2017, 82% of countries that currently issue physical identity cards have implemented eID programs, and by 2021, 3.6 billion people globally will possess some form of eID [1]. This trend traces back to Estonia, where the world's first national eID, known as the ID-kaart, was issued in 2002 [2]. Estonia's eID program was meant to offer a single, state-backed method for Estonians to authenticate their digital identity; prior to 2002, users had to use one of the various authentication schemes offered by major banks in Estonia to access third-party online services [3]. Since then, many other countries, predominantly European, have planned for or implemented eID [4]. eID is expected to revolutionize the delivery of government services, by making it more accessible and efficient: Citizens will be able to access government services online and use digital signatures to verify sensitive documents, including electronic voting ballots. eID can also be used by third-party services for user authentication, thus granting users more centralized control of their digital identities and encouraging transparency in how third-party services are accessing users' personal data. The inclusion of identity provision in the United Nations Sustainable Development Goals as target 16.9 [5] has also led development agencies to look at eID as a way "to build a robust and efficient identification system at a scale previously not as achievable" [6]. However, the security of eID systems must be considered by all countries with or planning to implement eID programs, now more than ever: Estonia was crippled by one of the world's largest instance of state-sponsored cyberattacks in 2007, and it discovered and fixed a cryptographic vulnerability affecting 750,000 eID users in August 2017. As cyberattacks become increasingly inevitable, individual countries must carefully weigh the potential vulnerabilities against the benefits of eID, for both the government and citizens, especially countries that implement eID for development purposes.

To the Community

It is crucial that the United States considers implementing a national eID program. Existing digital authentication methods using username-password combinations have been proven to be vulnerable to attacks, creating problems such as identity theft and fraud. The fragmented state of digital authentication platforms may also be encouraging users to adopt

weaker passwords that are easier to remember. Thus, a U.S. national eID program could potentially improve the integrity of digital information and transactions. The issue of eID may also be a partial answer to the attribution problem in cybersecurity, which highlights the current technical limitations to identifying the source or perpetrator of a cyberattack, be it a state or non-state actor [7]. A national eID program may help law enforcement agencies or businesses to identify the source of a cyberattack more easily, due to the digital footprints that the use of an eID will leave behind. While this identification may not lead directly to the mastermind behind the attack, it will be useful in helping cyberattack victims better understand and protect themselves against the threat.

However, as of 2018, the United States does not have a national eID program. There continues to be pushback from many states and civil rights groups on the Real ID Act of 2005 [8] — which implements federal requirements for physical identity cards — indicating the possibility of strong public opinion against the federal government imposing eID standards nationwide. At the same time, the Trusted Identities Group of the National Institute of Science and Technology's Applied Cybersecurity Division has been facilitating the private sector's leadership of the development of eID systems that the federal government may eventually adopt for both its internal and public use. This public-private partnership has led to the proliferation of private initiatives such as OAuth, OpenID, and SAML (Security Assertion Markup Language), but no governmental push to consider the feasibility of implementing eID.

On the other hand, Singapore, in its quest to build a 'Smart Nation,' announced the development of a national eID system in August 2017, while explicitly citing Estonia as an example to emulate. Among other features, Singapore's system includes a data vault that can be used across all public and select private digital services and digital signatures [9]. Unlike the United States, the Singapore government has not faced any public pushback against its plans. Nonetheless, it is still important for citizens of countries like Singapore, which are enthusiastic to implement eID, to weigh the benefits and potential vulnerabilities for themselves.

Return of Coppersmith's Attack (ROCA)

The most recent, and potentially most dangerous, vulnerability discovered in eID systems involved a flaw in an Infineon RSA public-key cryptography library that was discovered and disclosed in 2017. RSA — an asymmetric cryptosystem — generates public and private key-pairs based on the product of two large prime numbers; the security of RSA rests on the practical difficulty of factorizing that product into its constituent prime factors to reverse engineer the private decryption key. However, according to the researchers that discovered the flaw, a private key generated using the library can be attacked using brute-force in less than 3 months if the key is 1024-bit, and less than 100 years if the key is 2048-bit [10]. The attack was named Return of Coppersmith's Attack (ROCA), after a factorization method that the researchers adapted. After it was disclosed, it was listed in the Common Vulnerabilities and Exposures (CVE) database [11]. In fact, this vulnerability may be more familiar to the public as a flaw in Infineon-manufactured Trusted Platform Modules (TPM), which many Windows systems that rely on to generate cryptographic keys [12].

In September 2017, Estonia first announced that software installed on the chip embedded in identity cards issued for its national eID system suffered from this vulnerability [13]. Initially, the Estonian government downplayed the risks presented by this vulnerability, stating on a frequently asked questions page that "powerful and expensive computing power to calculate the secret key and special custom-made software for signing are also needed" [14]. In the interest of transparency and trust, the government also chose to publicly disclose the vulnerability, as soon as it was informed by the researchers who first discovered it and before a patch was ready [15]. Users of eID in Estonia were first asked to install an updated certificate on their eID, which now use a more secure elliptic-curve cryptosystem to generate key-pairs [16]. A month later, the Estonian government took the extraordinary step to suspend all 750,000 existing eID certificates that were affected by this vulnerability, such that users could only use their eID after they had installed the certificate update, after realizing that the ROCA vulnerability affected eID and computer systems worldwide and could thus be exploited by "international cybercrime networks" [17]. The decision to suspend was costly and disruptive, indicating the severity of the vulnerability to the eID system as assessed by the Estonian government: There were 750,000 affected Estonian eID cards that had to be remotely updated, out of a population of 1.3 million and an additional 30,000 e-residents [18]. Estonia also held its municipal elections in October 2017, in which 60.7% of the total number of votes were casted online, using the Estonian eID system for authentication [19].

While this vulnerability can be fixed with a software update, not all countries with a national eID system may act with the same level of transparency and urgency as Estonia. Apart from Estonia, few other countries have been forthcoming in the impact of this vulnerability on their respective eID systems [20]. While Spain acted swiftly to revoke all of the certificates on eID cards — known as Documento Nacional de Identidad electrónico (DNIe) — issued since 2015, it failed to issue any software updates for the certificates, and several users were apparently still able to use their eID on government services [21]. Slovakia — one of the examples cited in the original research paper — also moved to generate longer keys beyond 2048 bits that are resistant to the ROCA vulnerability. Additionally, while national governments may take steps to ensure the security of their eID systems, third-party services that have access to eID but use an unpatched TPM may expose eID systems to an attack exploiting this vulnerability.

To date, there is no information that the ROCA vulnerability has been exploited in a large-scale attack against any eID or computer system. There is a possible reason for this: The researchers who discovered this flaw practiced responsible disclosure by informing Infineon in February 2017 — eight months before a public disclosure, an appropriate but longer-than-usual amount of time given the seriousness of this vulnerability — and working with Infineon and major vendors on developing appropriate software patches [22]. Yet, another group of researchers was able to reconstruct an attack that was faster than what the original authors had described, even with just a limited public disclosure in October 2017. They noted that a limited amount of publicly-available information may have lulled users into a false sense of security, while the delay in releasing the full details of the flaw may have hurt, rather than helped, security. Their "best guess is that serious attackers found the Infineon vulnerability years ago and have been quietly exploiting it since then" [23].

General Coppersmith's Attack

Previously, in 2013, researchers had found the "first successful public application" of Coppersmith's attack — the inspiration behind the ROCA vulnerability — in Taiwan's eID system. The research team found a remarkable loss of entropy in existing 1024-bit public and private key-pairs, such that 184 keys were broken in mere hours by using a combination of calculating the greatest common divisor between number pairs and Coppersmith's attack to discover the prime factors that underwrote the security of this system [24]. Although 184 keys out of a database of two million may seem miniscule, any number of flawed keys is too much for a cryptosystem that is supposed to offer watertight security for a national eID program. If attackers could use even just one of the broken keys for impersonation, the confidentiality and/or integrity of the Taiwanese eID system would already have been violated.

This group of researchers also practiced responsible disclosure to the Taiwanese government a few months before the publication of the paper. The government, which said that the flaw may have affected up to 10,000 identity cards manufactured by Taiwanese firm Chunghwa Telecom [25], immediately acted to trace and replace all affected cards, and revoke all compromised eID certificates. The researchers noted that this response may be inadequate because a flawed random number generator may "sometimes manifest themselves as primes that appear only once, such as the primes that [they] found by Coppersmith-type attacks," and instead recommended that the Taiwanese government revoke all certificates that have used this flawed generator and replace with a more robust random number generator [24]. Such an attack may be less dangerous than the more recently-discovered ROCA vulnerability, since it only applies in instances of poorly-generated key-pairs. On the other hand, the ROCA vulnerability applies to all chips that are equipped by the vulnerable Infineon library, regardless of how robust the rest of the system may be.

Certifications: False Sense of Security

The researchers of the Taiwanese eID flaw noted that the discovery of this flaw — while not a vulnerability that affects all computer or eID systems in general — signifies the possibility that there may be more eID or digital certificate systems that have weak random number generators that produce numbers with shared prime factors. In this instance, the Taiwanese government had declared that its eID system passed the Level 2 requirements of the FIPS 140-2 Security Requirements for Cryptographic Modules [26], but yet it still had a fatal flaw. The discovery of this flaw may indicate that the certification system in cryptography — and more broadly, cybersecurity — is broken; the certification checks in this case did not check for the quality of the random number generator, thus allowing the eID system to be certified even with the presence of a flaw.

Similarly, the Infineon library where the ROCA vulnerability was discovered had been declared to have passed the requirements of various certification authorities, including the Federal Office for Information Security in Germany [27] and Common Criteria standards [28]. Estonian authorities also stated that "the compliance of the ID card and the chip with security requirements has been certified by the competent German and French certification bodies" [14].

The researchers who discovered the ROCA vulnerability identified that the current industry certification process rewards security by obscurity, without considering the trade-off between the difficulty for attackers to spot a flaw and the unknown impacts of the flaw due to a later discovery by security researchers [10]. A broken certification system, as shown in how the ROCA flaw slipped through an extensive certification process, creates a deficit of trust in the current security certification framework and in the systems that it certifies as secure.

Action Items

For countries that already have implemented national eID programs, they should be transparent in how a publicly-disclosed weakness or vulnerability affects their system. Estonia's response to the disclosure of the ROCA vulnerability offers an example for other countries to emulate, while the responses of countries like Spain, Slovakia, Taiwan leave much to be desired. Estonia may have been forced to be transparent because of its growing e-Residency program, that allows non-residents to apply for an Estonian eID and access Estonian public and private services online, thus facilitating business and trade in the broader European community [18]. However, other countries without similar e-Residency programs should also be upfront with their citizens about how disclosed vulnerabilities affect their computer systems, so that citizens can be reassured that their personal information and digital identities are being safeguarded, and the confidentiality and integrity of the eID system is preserved.

Countries can also consider investing into greater cybersecurity research on the cryptosystems that underwrite all digital identity and authentication systems. In the case of ROCA, the researchers were funded by the Czech Science Foundation, while the researchers who discovered the successful application of a Coppersmith's attack on Taiwan's eID system were funded by the Taiwanese, Dutch, and American science research foundations. Proactive investment into research can be a form of defense, in that countries are able to discover flaws earlier than attackers do, and thus disclose the vulnerability and release a patch without a long delay.

As of now, there is no country that publicly discloses the full database of the public keys of all its eID users. However, Estonia offers a "lookup [service] with significant limitations on the number of queries allowed" [10], which researchers were able to utilize in order to estimate the impact that the ROCA vulnerability has on the Estonian eID system. Inevitably, malicious actors can also use such publicly-disclosed information to research and exploit vulnerabilities in not just national eID systems, but national government systems in general. Countries that have implemented national eID programs need to consider the trade-off between being accountable through transparency and being secure through obscuring.

For countries that are considering the implementation of eID, the recent discoveries of flaws in cryptographic systems will indicate to them that the security of an eID system is not merely ensured by keeping their citizens' data secure and private. Instead, countries implementing eID must closely examine the cryptosystems — in both the physical identity card and the digital services — that they will be using for potential vulnerabilities or weaknesses. The development of Estonia's, and many other countries', eID program is contracted out to Gemalto,

but it is important that countries do not outsource the concern that they should have for the security of their own computer systems. Countries must weigh the vulnerabilities against the benefits of implementing eID systems; however, rather than merely treat the risks as hypothetical, countries should treat the existence of vulnerabilities and the threat of exploitations as a foregone conclusion. As researchers have pointed out with the discovery of the ROCA vulnerability, an optimistic view is that the vulnerability has already been used, albeit silently, by attackers.

For countries that are dealing with future disclosures of vulnerabilities that affect eID, they should consider taking a remedial measure that does not just revoke the eID certificates that have been proven to vulnerable, but to treat the entire system as vulnerable. This mindset — unlike the one adopted by the Taiwanese government in 2013 — will prompt countries to overhaul a vulnerable system completely, rather than only remove the instances of output that demonstrate the existence of a system flaw.

For all members of the cybersecurity community at large, the current framework of certification needs to be reexamined. Not only does certification not entail a robust check for a system's integrity and full functionality, but it also is sometimes abused by hardware and software manufacturers in marketing their products disingenuously. While there is no evidence to suggest that Infineon intentionally created a flaw in generating keys for its cryptosystem, or that Taiwan intentionally generated numbers that had poor entropy and could be reverse-engineered, these systems' certifications are now worthless considering their (newly-) discovered flaws. A revamped certification framework should not reward obscurity over transparency. It should also drop its current culture of secrecy by being transparent in the methods and results of determining the security of a computer system or product.

Conclusion

With identity now a cornerstone of global development policies, it is likely that an increasing number of countries will look towards the success stories of countries such as Estonia in implementing a national eID program. However, caution should be exercised. The flaws that have been discussed barely scratch the surface of security issues that exist in eID, and currently exclude some of the more commonly-discussed issues surrounding user privacy and the security of end-users' own computer systems on which eID services are accessed. In looking at three specific vulnerabilities in great detail — including two specific cryptographic flaws based on Coppersmith's attack and a more general weakness pertaining to security certifications — this paper has sought to demonstrate to readers the sheer complexity of securing eID systems.

References

[1] Gemalto, “National ID cards: 2016-2018 facts and trends,” *Gemalto*, 03-May-2018. [Online]. Available: https://www.gemalto.com/govt/identity/2016-national-id-card-trends. [Accessed: 06-May-2018].

[2] M. Pedak, “eID: Estonian experience,” e-Governance Academy, Tallinn, Estonia, Dec. 2013.

[3] T. Martens, “Electronic identity management in Estonia between market and state governance,” *IDIS*, vol. 3, no. 1, pp. 213–233, Jul. 2010.

[4] M. Pala, “Countries with electronic ID cards for secure identification,” *Smart ID*, 26-Apr-2017. [Online]. Available: https://smartid.ee/countries-available-smart-card-identifications-methods/. [Accessed: 06-May-2018].

[5] United Nations, “Goal 16 .:. Sustainable Development Knowledge Platform,” *Sustainable Development Goal 16: Targets & Indicators*. [Online]. Available: https://sustainabledevelopment.un.org/sdg16. [Accessed: 07-May-2018].

[6] “Identification for Development: Strategic Framework,” World Bank Group, Jan. 2016.

[7] InfoSec Institute, “The Attribution Problem in Cyber Attacks,” *InfoSec Resources*, 01-Feb-2013. [Online]. Available: http://resources.infosecinstitute.com/attribution-problem-in-cyber-attacks/. [Accessed: 07-May-2018].

[8] Electronic Frontier Foundation, “Real ID.” [Online]. Available: https://www.eff.org/issues/real-id. [Accessed: 07-May-2018].

[9] K. Kwang, “National Digital Identity system to be cornerstone of Singapore’s Smart Nation vision,” *Channel NewsAsia*, Singapore, 20-Aug-2017.

[10] M. Nemec, M. Sys, P. Svenda, D. Klinec, and V. Matyas, “The Return of Coppersmith’s Attack: Practical Factorization of Widely Used RSA Moduli,” in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, New York, NY, USA, 2017, pp. 1631–1648.

[11] “CVE-2017-15361,” *Common Vulnerabilities and Exposure*. The MITRE Corporation, 15-Oct-2017.

[12] Microsoft, “ADV170012 | Vulnerability in TPM could allow Security Feature Bypass,” *Security TechCenter*, 11-Jan-2018. [Online]. Available: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV170012. [Accessed: 08-May-2018].

[13] D. Goodin, “Millions of high-security crypto keys crippled by newly discovered flaw,” *Ars Technica*, 16-Oct-2017.

[14] Estonia Information Systems Authority, “Frequently Asked Questions > How to use safely > ID-CARD > ID.ee.” [Online]. Available: https://www.id.ee/index.php?id=38066. [Accessed: 08-May-2018].

[15] K. Korjus, “We told you about a potential security vulnerability. Here’s our update.,” *E-Residency Blog*, 04-Oct-2017.

[16] K. Korjus, “Estonia is enhancing the security of its digital identities,” *E-Residency Blog*, 31-Oct-2017.

[17] K. Korjus, “Digital ID cards now only work with new certificates,” *E-Residency Blog*, 03-Nov-2017.

[18] A. Rang, “Who are Estonia’s e-residents?,” *E-Residency Blog*, 30-Nov-2017.

[19] “Advance voting closes, turnout at 27.8 percent, new e-voting record,” *ERR*, 12-Oct-2017.

[20] Z. Marzouk, “Ex-Estonian president: Other countries staying silent over digital ID flaws,” *IT PRO*, 14-Nov-2017.

[21] J. Leyden, “Confusion reigns over crypto vuln in Spanish electronic ID smartcards,” *The Register*, 15-Nov-2017.

[22] “ROCA: Vulnerable RSA generation (CVE-2017-15361) [CRoCS wiki].” [Online]. Available: https://crocs.fi.muni.cz/public/papers/rsa_ccs17. [Accessed: 08-May-2018].

[23] D. J. Bernstein and T. Lange, “Reconstructing ROCA,” *The cr.yp.to blog*, 05-Nov-2017.

[24] D. J. Bernstein *et al.*, “Factoring RSA Keys from Certified Smart Cards: Coppersmith in the Wild,” in *Advances in Cryptology - ASIACRYPT 2013*, 2013, pp. 341–360.

[25] D. Goodin, “Fatal crypto flaw in some government-certified smartcards makes forgery a snap,” *Ars Technica*, 16-Sep-2013.

[26] National Institute of Standards and Technology, “Security requirements for cryptographic modules,” National Institute of Standards and Technology, Gaithersburg, MD, NIST FIPS 140-2, May 2001.

[27] Infineon Technologies AG, “Background Information on software update of RSA key generation function,” *Infineon*. [Online]. Available: https://www.infineon.com/cms/en/product/promopages/rsa-update/rsa-background. [Accessed: 08-May-2018].

[28] I. Schubert, “ROCA: BLAMING INFINEON IS THE EASY WAY OUT,” *RSA.com*, 26-Oct-2017.