Lecture 5

Secure Online Transactions

Outline

- Background
- SingPass
- National Authentication Framework
- Guest speaker: Mr. Chai Chin Loon

  Chief Operating Officer

  Assurity Trusted Solutions Pte Ltd

Background

Background

- Authentication
  - A process of validating a person's identity for security purposes

- 3 recognised factors of authenticating individuals
  - "Something you know" (e.g., password or PIN)
  - "Something you have" (e.g., hardware security token, OTP via SMS)
  - "Something you are" (e.g., finger print, a retina scan or other biometric)

Hardware Security Tokens

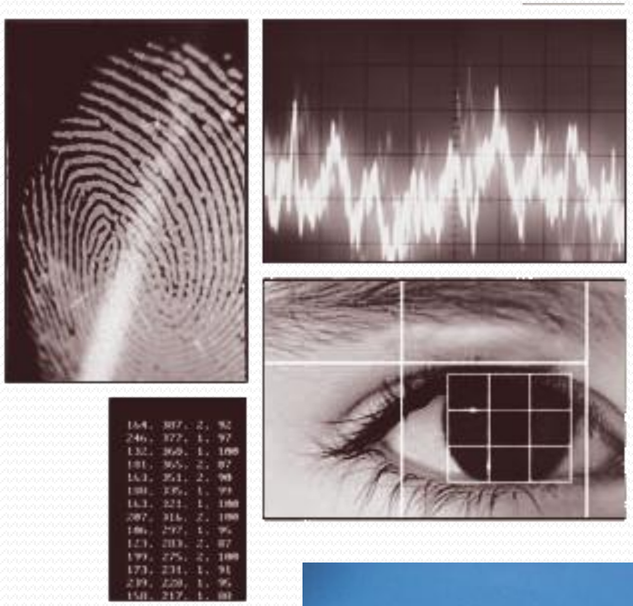
- Dynamically-generated passwords delivered via hardware tokens

SMS Authentication

- Designed to complement password log-ins
- User must confirm with one-time password sent through SMS to his/her cell phone
  - Valid once & expires after a fixed time
- Pros
  - Leverages a device user already owns
  - Easier to manage than tokens & relatively inexpensive
  - Likely to notice immediately if cell phone is lost
- Cons
  - SMS may be intercepted by cyber criminals using forwarding services to hijack info to their phones

Biometrics

- Every human has unique physiological attributes
  - Examples: fingerprint, iris or retina scan
- Registered biometric sample is compared against a newly captured sample
- Can be extremely accurate identification solution



Strong Authentication

- A system is said to use strong authentication when it requires at least 2 of 3 factors before access to system is granted

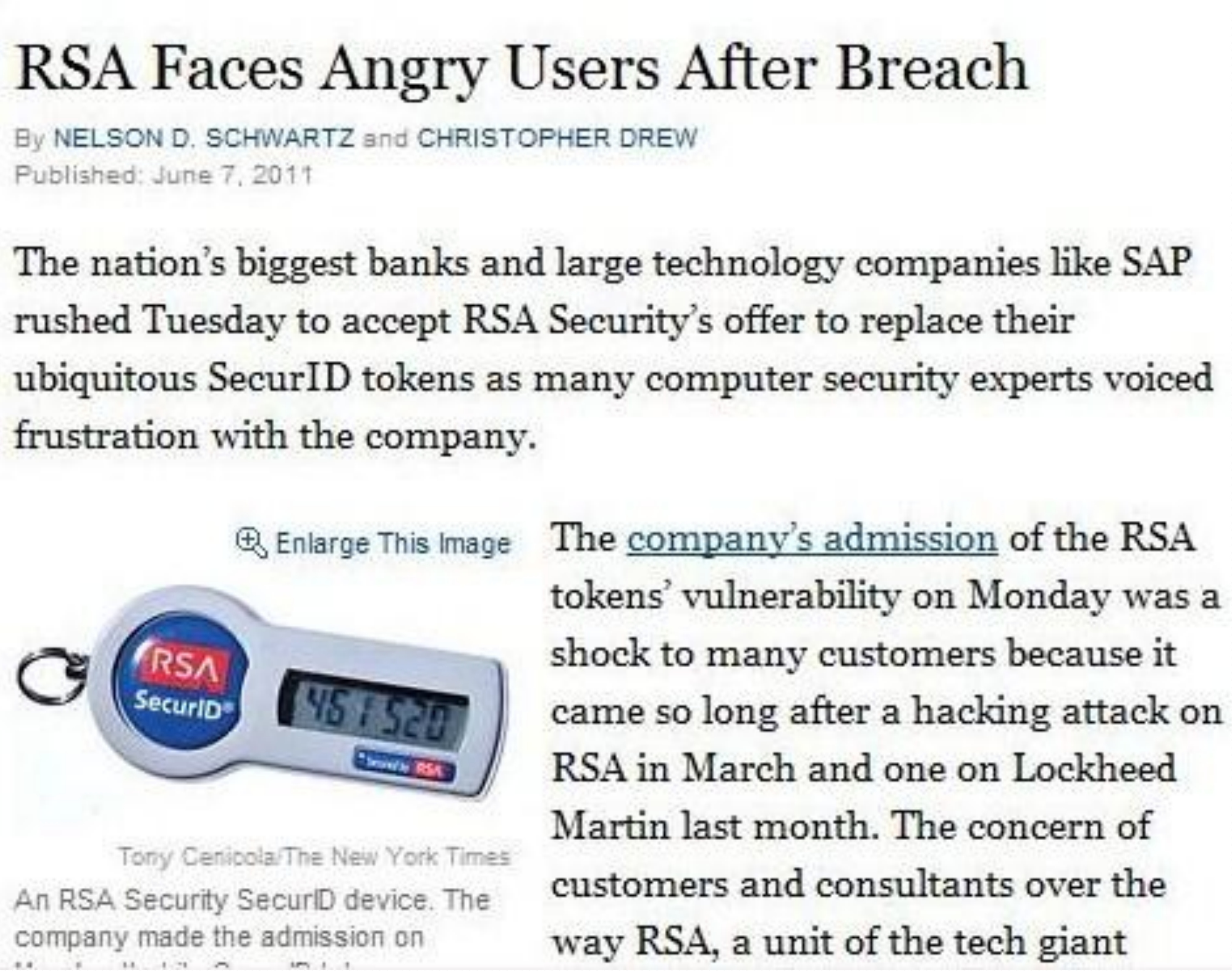
- Traditional single-factor authentication requires only one authentication factor (normally knowledge of a password) in order to gain access to a system

2nd Factor Authentication (2FA)

- A more rigorous process of validating identities
- Popular 2FA method
  - Banks offer One-Time Password (or OTP) to their online consumers
- When a user accesses an online service, s/he enters
  - User-ID & Password
  - “second factor password” generated on demand

2FA (2/2)

- Dynamically-generated “second factor password” could be delivered through
  - Token (hardware or software)
  - Via SMS
  - Certificates
  - Biometrics
- Service providers (SPs) today deploy their own 2FA infrastructure
  - Authentication device or method tends to be proprietary
  - Can only be used to access specific online services



RSA Faces Angry Users After Breach

By NELSON D. SCHWARTZ and CHRISTOPHER DREW

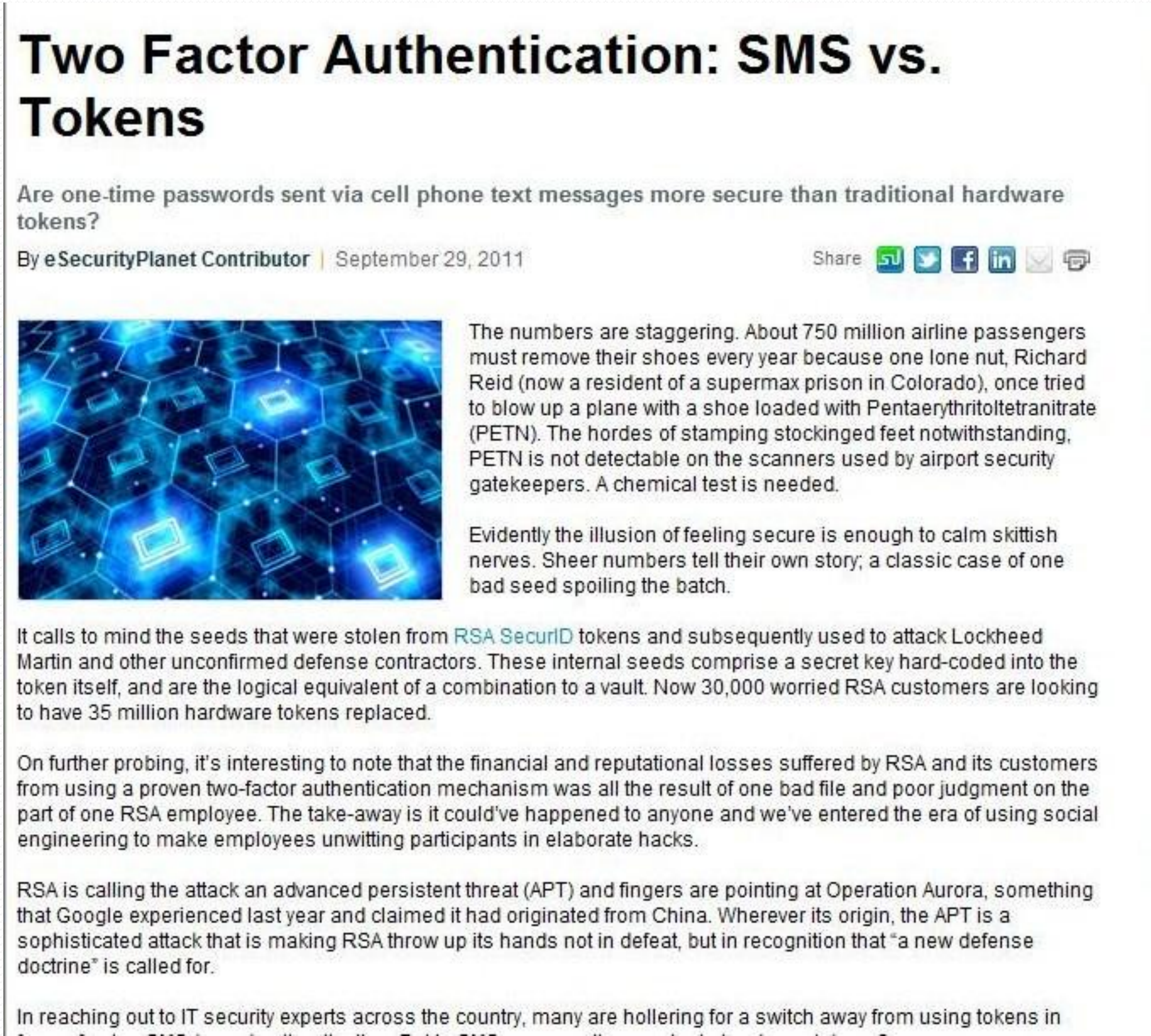
Published: June 7, 2011

The nation's biggest banks and large technology companies like SAP rushed Tuesday to accept RSA Security's offer to replace their ubiquitous SecurID tokens as many computer security experts voiced frustration with the company.

Tony Cenicola/The New York Times

An RSA Security SecurID device. The company made the admission on

The company's admission of the RSA tokens' vulnerability on Monday was a shock to many customers because it came so long after a hacking attack on RSA in March and one on Lockheed Martin last month. The concern of customers and consultants over the way RSA, a unit of the tech giant



Two Factor Authentication: SMS vs. Tokens

Are one-time passwords sent via cell phone text messages more secure than traditional hardware tokens?

By eSecurityPlanet Contributor | September 29, 2011

The numbers are staggering. About 750 million airline passengers must remove their shoes every year because one lone nut, Richard Reid (now a resident of a supermax prison in Colorado), once tried to blow up a plane with a shoe loaded with Pentaerythritoltetranitrate (PETN). The hordes of stamping stockinged feet notwithstanding, PETN is not detectable on the scanners used by airport security gatekeepers. A chemical test is needed.

Evidently the illusion of feeling secure is enough to calm skittish nerves. Sheer numbers tell their own story; a classic case of one bad seed spoiling the batch.

It calls to mind the seeds that were stolen from RSA SecurID tokens and subsequently used to attack Lockheed Martin and other unconfirmed defense contractors. These internal seeds comprise a secret key hard-coded into the token itself, and are the logical equivalent of a combination to a vault. Now 30,000 worried RSA customers are looking to have 35 million hardware tokens replaced.

On further probing, it's interesting to note that the financial and reputational losses suffered by RSA and its customers from using a proven two-factor authentication mechanism was all the result of one bad file and poor judgment on the part of one RSA employee. The take-away is it could've happened to anyone and we've entered the era of using social engineering to make employees unwitting participants in elaborate hacks.

RSA is calling the attack an advanced persistent threat (APT) and fingers are pointing at Operation Aurora, something that Google experienced last year and claimed it had originated from China. Wherever its origin, the APT is a sophisticated attack that is making RSA throw up its hands not in defeat, but in recognition that "a new defense doctrine" is called for.

In reaching out to IT security experts across the country, many are hollering for a switch away from using tokens in

SingPass

- Objective
  - One authentication system to access all government e-services requiring single-factor authentication

- SingPass stands for Singapore Personal Access
  - Used where only one password needs to be provided when transacting with Government

- Since 1 March 2003, all Singapore residents aged 15 & above can apply for a SingPass ID/password, if they do not already have one, for the purpose of transacting with Government via online e-services

SingPass authentication system

- Strives to provide users with a high level of confidence by allowing an alphanumeric password that can be as long as 24 characters, to enable end-to-end encryption of user IDs & passwords, thereby promising a high level of availability & resiliency

- Enhances internal Government efficiency by eliminating need for each agency to develop & administer its own authentication system

Usage

- 57 government agencies use SingPass as a form of authentication for citizens & residents to access more than 270 e-services that require secure user identification
- Since its launch, total volume of SingPass authentication transactions increased from 4.5M in 2003 to 40M in 2010
  - Represents more than 8x increase over 7 years

SingPass Users

- SingPass system today has more than 2.8M registered users

- Eligible users to apply for SingPass
  - Singapore Citizens & Permanent Residents
  - Employment Pass & Personalised Employment Pass holders
  - EntryPass holders
  - S-Pass holders
  - Dependant Pass holders (of EP, PEP, EntrePass & S-Pass holders)
  - Selected Work Permit holders

Examples of government e-services using SingPass (1/4)

- **Accountant’s General Department**
  - Vendors @ Gov

- **Accounting & Corporate Regulatory Authority**
  - Local or Foreign Company Names Application
  - Conversion of Companies to Limited Liability Partnerships
  - Changes in Particulars of Businesses
  - Purchase of Business Profile

Examples of government e-services using SingPass (2/4)

- **Central Provident Fund Board**
  - My Statement
  - Track retirement planning at Retirement Ready @ my cpf
  - Transfer of CPF Savings from Ordinary Account to Special Account, & topping-up of CPF Minimum Sum
  - e-Submission for Employers

- **Housing & Development Board**
  - My HDBPage

Examples of government e-services using SingPass (3/4)

- **Infocomm Development Authority**
  - Infocomm Competency Management System
- **Inland Revenue Authority of Singapore**
  - e-Filing for individual income tax
  - GST Filing for companies
- **Intellectual Property Office of Singapore**
  - e-TradeMarks
- **Media Development Authority**
  - Application for TV/Radio Licence

Examples of government e-services using SingPass (4/4)

- **Ministry of Defence**
  - The NS Portal
- **Ministry of Finance**
  - GeBIZ
- **Ministry of Manpower**
  - Application for Work Permit by employers and businesses
  - Access to Foreign Worker Levy Billing
- **Ministry of Trade & Industry**
  - Online Business Licensing Service (OBLS)
- **Urban Redevelopment Authority**
  - E-services for Licensed Developers
  - Application, extension & renewals for Change of Use

National Authentication Framework

National Authentication Framework (NAF)

- Seeks to realise vision of iN2015 masterplan for a secure & trusted enabling infocomm infrastructure that can facilitate delivery of online services offered by public & private sectors
- With increased availability of online services offered by key sectors (such as banking & finance, Government & healthcare), NAF can safeguard against unauthorised access to sensitive info available online (such as bank account details, securities trading account details or electronic health records)

Goals of NAF

- Nationwide common platform for strong authentication that
  a) Enables consumers to enjoy convenience of using a single authentication device to access multiple online services that require strong authentication
  b) Enables businesses to enjoy cost savings when they leverage on NAF instead of implementing their own strong authentication systems
  c) Boosts online trust & confidence, thus helping to entrench Singapore's status as a trusted infocomm hub
  d) Enhances protection against online identity theft for online services for both consumers & online business owners

NAF Implementation

- A nationwide strong authentication infrastructure that provides consumers greater assurance when performing online transactions
- Government's 2FA system is meant to supplant clutter of tokens issued separately by service providers like banks & stock broking firms
- In 2012, Singaporeans will be given an advanced password token for securing their online transactions

Australian National e-Authentication Framework (NeAF)

From recommended reading

Scope of NeAF

- Electronic authentication of identity of individuals & businesses
- Authentication of government websites

NeAF provides

- Principles to determine & implement a-Authentication approaches
- 5 e-Authentication assurance levels & a recommended set of criteria to determine level of assurance for a particular e-transaction
- An approach to determine e-Authentication solution required to satisfy the e-Authentication assurance level
- An approach to validate e-Authentication approach selected

Key Principles Underpinning NeAF Application (1/3)

- Transparency
  - Consultation with relevant stakeholders
- Risk Management
  - Ensure selection of e-Authentication mechanisms
- Consistency
  - In selecting a-Authentication mechanisms
- Interoperability
  - Facilitates interop & compliance with relevant standards

Key Principles Underpinning NeAF Application (2/3)

- Responsiveness & accountability
  - Respond to individuals’ & business’ needs
  - Provide guidance on use & provide dispute handling processes
  - Accountable in determing & addressing specific issues
- Trust & confidence
  - Enable balance between usefulness & security
- Privacy
  - Collect, use & disclosed info in accordance with laws

Key Principles Underpinning NeAF Application (3/3)

- Choice
  - Ability to use one or more electronic credentials to access services across multiple organisations
- Flexibility
  - Supports range of fit-for-purpose e-Authetication approaches
- Cost effectiveness & convenience
  - E-Authentication processes are seamless & simple
  - Allow reuse of existing e-Authetication credentials

Guest Speaker

Mr. Chai Chin Loon

Chief Operating Officer

Assurity Trusted Solutions Pte Ltd