The March 2011 RSA Hack

What is SecurID?

- Two-factor authentication protocol

Most common example of TFA: ATM authentication

Token

a. ???
b. ???

?

a. ATM Card
b. PIN code

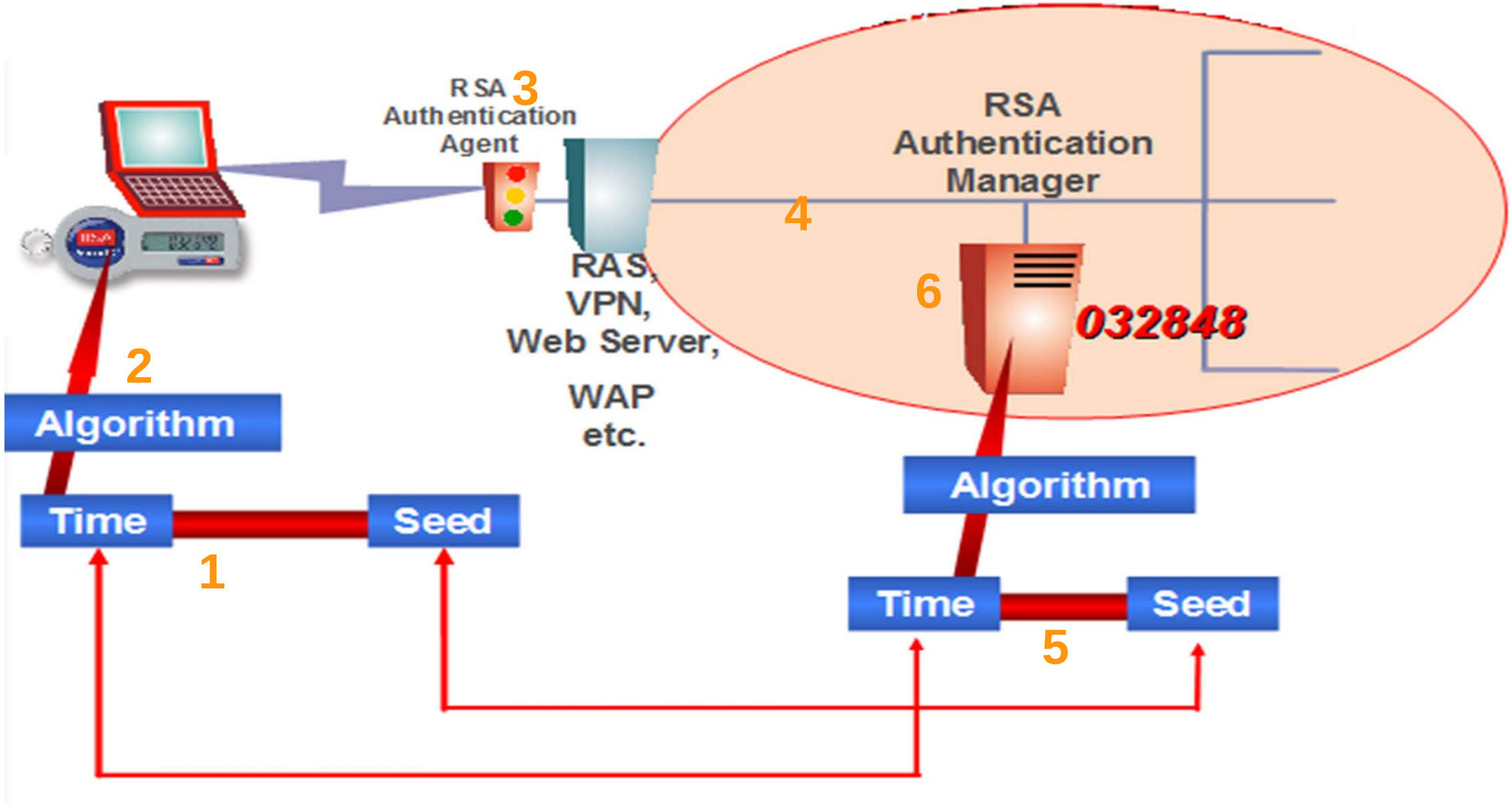
How does SecurID work?

- Provides two-factor authentication by producing one-time passwords
- Passwords change automatically every 30 or 60 seconds and are valid only for this duration
- End-user authenticates himself by providing
  - username
  - passcode = password + Token code

User Credentials

- Each token associated with a unique 128 bit random key (seed)
  - factory-encoded
- Customer authenticating systems check credentials
- →RSA server checks token validity

How does SecurID work?



H(seed,time,serial) = token code

Who uses SecureID ?

- Over 40 millions users world-wide

So....

So SecureID is safe .....right??

YES....under two assumptions

- The underlying cryptographic functions are "hard" to break
  - AES implementation
- The Seeds of the tokens remain secret
  - Human factor

So...

~~What was stolen from RSA?~~

What could have been stolen from RSA?

- Token Seeds (*schneier.com*)
- Source code of implementation (*hbarel.com*)
- Master/Root key for Seed Generation (*darkreading.com*)

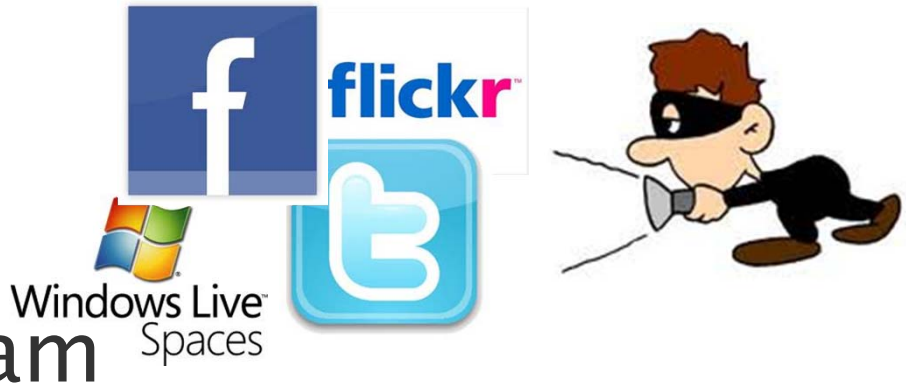
***a posteriori* observation**

Somewhere within RSA servers resided information on SecurID sufficient enough to cause trouble in case of

The Hack...

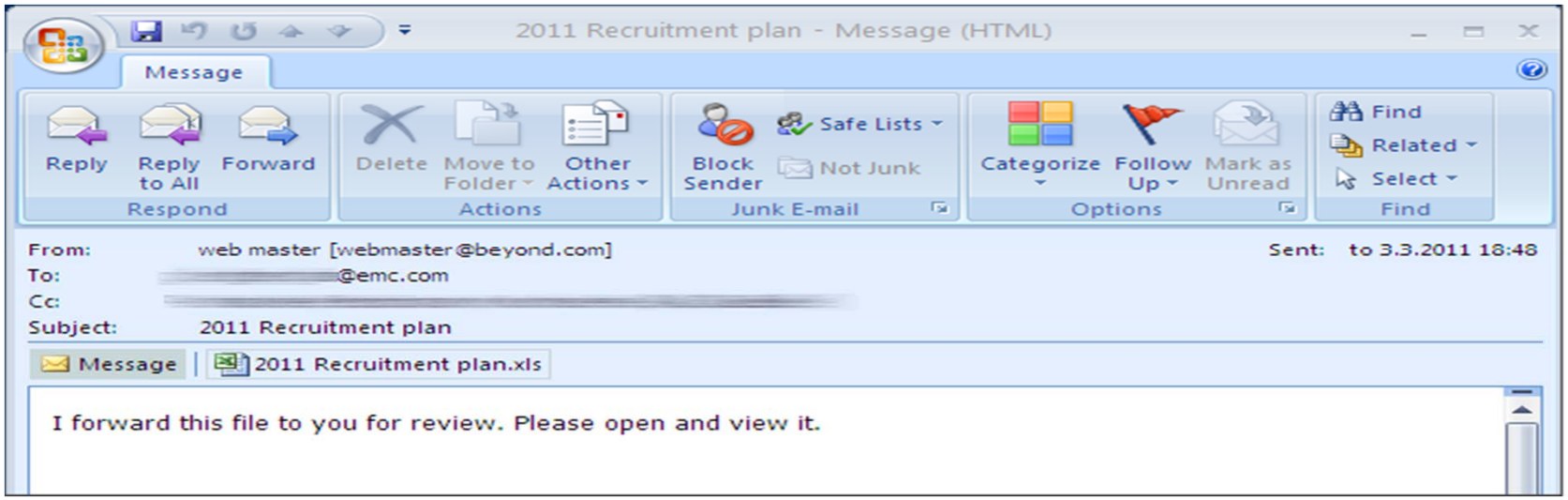
Part 1: Homework

- "Social Engineering"



- Targeted Phising Scam

- Phising e-mail titled "Recruitment Plan 2011"



The Hack...

Really?? Just an e-mail scam???

From: webmaster@beyond.com	Beyond is a partner known to RSA employees
To: 1 RSA employee Cc: 3 more RSA employees	Cleverly addressed to one person, with more targets on CC, looks less like SPAM
Subject: 2011 Recruitment Plan	Subject of interest to HR and Managers
Body: I forward this file for you to review. Please, open and view it.	Too simple to look real, even accounting for current trends to simplify communication
Attachment: 2011 Recruitment Plan.xls	

✓ Classified as SPAM → ended up in the Junk folder

✗ At least one user found it interesting enough to retrieve it...

The Hack...

Part 2: Breaking-in

- Attached Excel spreadsheet with embedded Flash object which is executed by Excel(why???)...
- SWF utilizes CVE-2011-0609 Adobe Flash vulnerability → access the kernel and install Poison Ivy RAT (remote-access-tool)
- Poison Ivy set in reverse-connect mode → PC reaches out to the C&C over port 80 rather than the other way around. (outbound traffic over dedicated ports harder to control)

Key-Point → Attack was zero-day at the time!! Adobe issued a patch addressing the above problem shortly after the RSA breach...

The Hack...

Part 3: Grab the money and run!

- Monitor inbound and outbound traffic (digital shoulder surfing)
- Privilege escalation → Higher ranking employee accounts
- Locate particular resources of importance (SecureID seeds)
- Aggregate and encode information
- Output information via FTP to server good.mincesur.com (physically located in China)
- Stolen info sto[illegible]ble to locate once offline

Aftermath

- RSA characterized it as APT

APT ???

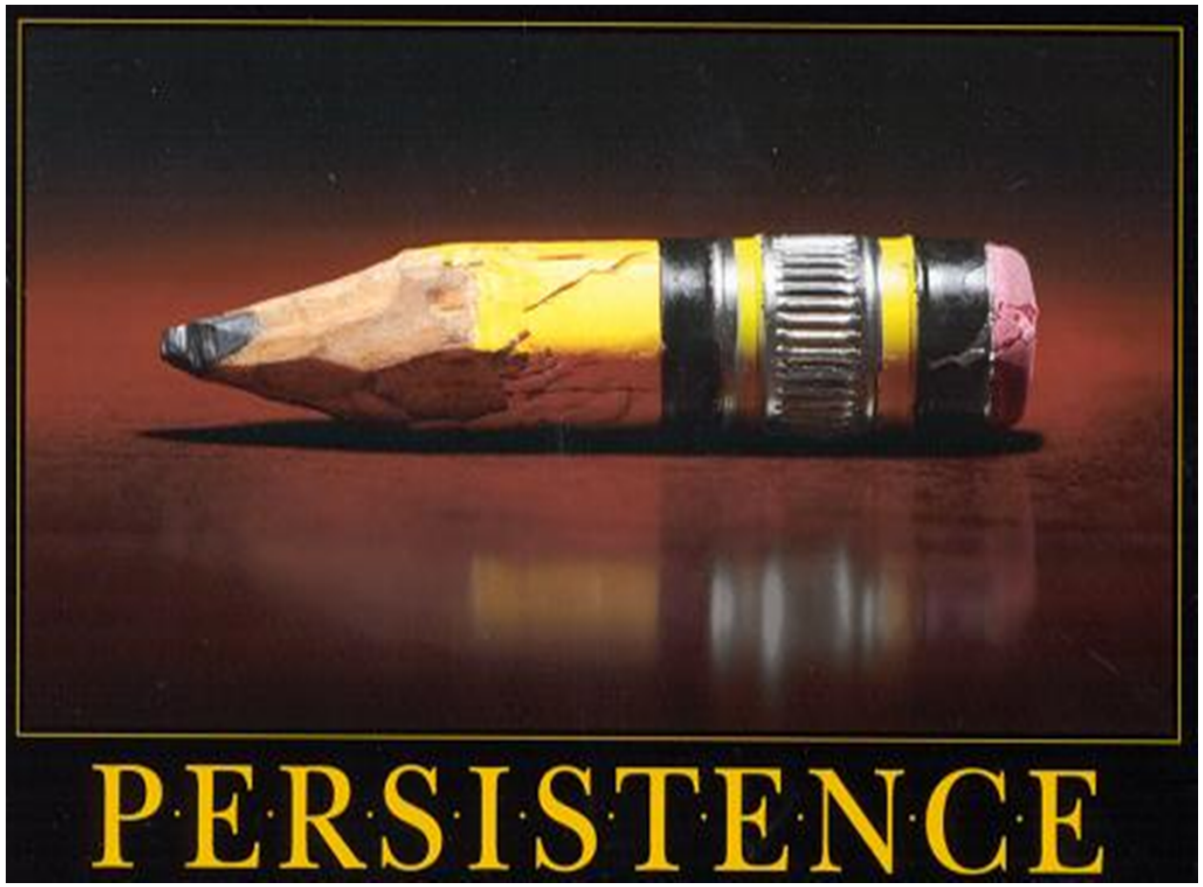
Advanced

using elaborate up-to-date techniques, possibly created for this particular attack

APT ???

Persistent

attacker determined and dedicated to spend great amount of resources (time, money, computational power) to deploy techniques against this **particular** *organization (even bribery, infiltration etc..)*



APT ???

Threat

attacker wants to compromise company assets, access enterprise information and generally harm the organization/company economically or otherwise

Aftermath

- RSA characterized it as APT
  - Similar to the one against Google(Operation Aurora) in 2009
  - Possibly nation-state launched?
  - Motivating research on new defense mechanisms against APT's
  - Rethink how we train and prepare employees for such scenarios
- Total (published) cost for RSA ~ $60 million!
  - Part of which relates to replacing SecurID tokens
- Attack on a security vendor → Compromises all of its customers

The Lockheed-Martin Attack

- Primary defense contractor of US and numerous other countries
- F-16, F-22, C-130 etc.
- In 2009, 7.1% of the funds handed out by Pentagon went to LM
- On May 28th 2011 Lockheed Martin Corp. was hit by an unspecified cyber-incident

Anonymous source from within LM: "Attackers exploited LM's VPN access system, which allowed RSA SecurID remote log-on. They apparently possessed the seeds as well as serial numbers and the underlying

Thank you...

References/Bibliography

- Uri Rivner - “Anatomy of an Attack” *http://blogs.rsa.com/rivner/anatomy-of-an-attack/*
- Schneier on Security - “Details of the RSA hack” *http://www.schneier.com/blog/archives/2011/08/details_of_the.html*
- Mikko Hypponen - “How We Found the File That Was Used to Hack RSA” *http://www.f-secure.com/weblog/archives/00002226.html*
- A Websense White Paper - “Advanced Persistent Threats and other Advanced Attacks” *http://www.websense.com/assets/white-papers/advanced-persistent-threats-and-other-advanced-attacks.pdf*
- RSA confirms its tokens used in Lockheed hack *http://gcn.com/articles/2011/06/07/rsa-confirms-tokens-used-to-hack-lockheed.aspx*
- Rodrigo Branco - “Into the Darkness: Dissecting Targeted Attacks” *https://community.qualys.com/blogs/securitylabs/2011/11/30/dissecting-targeted-attacks*
- AES SecurID Token *http://www.velocityreviews.com/forums/t367596-aes-securid-token.html*
- RSA Security presentation: An Introduction to RSA SecurID - *RSA SecurID.ppt*
- *Anatomy of Ownage.ppt* – NASA IT Summit Linton
- San Jose State University,Elen Stuart - *RSA SecurID Authentication.ppt*