Champlain College
Center for Digital Investigation

Vermont Bankers Association

# Two-Factor Authentication for Online Banking Applications

**Gary C. Kessler**
Champlain College
Center for Digital Investigation

Vermont Banking Association

10 May 2006

http://digitalforensics.champlain.edu/htcia

# Overview

- Online banking: Features and risks
  - » Phishing demo
  - » DNS cache poisoning demo
- FFIEC Guidance Overview
- Authentication methods
  - » Two-factor authentication
  - » Options for online banking
- Is two-factor authentication the correct approach?

© 2006, Gary C. Kessler 

# Online Banking: Features and Risks

© 2006, Gary C. Kessler


# Why Online Financial Services?

- Online banking is fastest growing service on the World Wide Web
  - » All banks are the same size on the Web
  - » Consumers get 24/7/365 access to financial info
    - We've all become bank tellers!
  - » Financial institutions are perceived as providing better customer service and save money
    - Bank branch: $1.07/transaction
    - Telephone banking: $0.55/transaction
    - ATM machine: $0.27/transaction
    - Internet banking: $0.01/transaction

© 2006, Gary C. Kessler

**Growth in online banking 2002-2004**

*The percentage of those in each group with internet connections who have tried online banking. In other words, 31% of online men had done online banking in October 2002 and 29% of online women had done it.*

| | *October 2002 N=1027 internet users* | *November 2004 N=537 internet users* |
|---|---|---|
| All internet users | 30% | 44% |
| Sex | | |
| Men | 31% | 49% |
| Women | 29% | 39% |
| Age | | |
| Generation Y (ages 18-27) | 29% | 38% |
| Generation X (ages 28-39) | 34% | 60% |
| Younger Baby Boomers (ages 40-49) | 33% | 42% |
| Older Baby Boomers (ages 50-58) | 26% | 49% |
| Household income | | |
| Live in households earning less than $30,000 | 21% | 32% |
| $30,000-$49,999 | 31% | 44% |
| $50,000-$74,999 | 33% | 51% |
| $75,000 or more | 35% | 55% |
| Educational attainment | | |
| High school graduate | 27% | 42% |
| Some college | 27% | 41% |
| College and graduate school degree | 37% | 52% |
| Internet connection at home | | |
| Dial-up | 24% | 35% |
| Broadband | 35% | 63% |

*Source: Pew Internet & American Life Project Surveys: Oct 7-27, 2002 (margin of error is±3%); Nov. 23-30, 2004 (margin of error is ±5%).*

© 2006, Gary C. Kessler 

# More Statistics...

- 40M online banking customers in U.S. in 4Q2005
  - » Up 27% from 4Q2004
- 36% increase in online bank bill payment customers in 2005
  - » Accounts for 25% of all online bill payments
  - » Bank of America has 5.1M active online bill payment customers (>50% of total)
  - » 37% of CitiBank's online banking customers use their online bill payment services; 34% of BofA customers

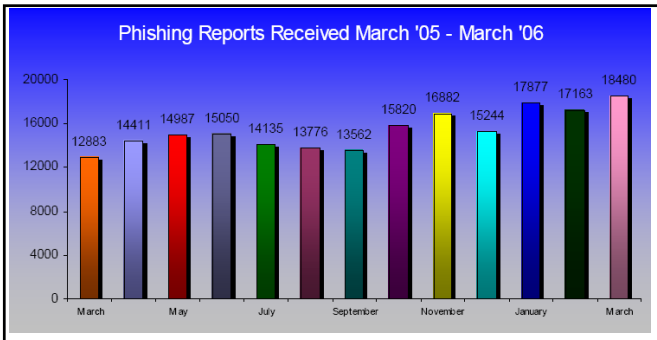
**Source: comScore Networks**

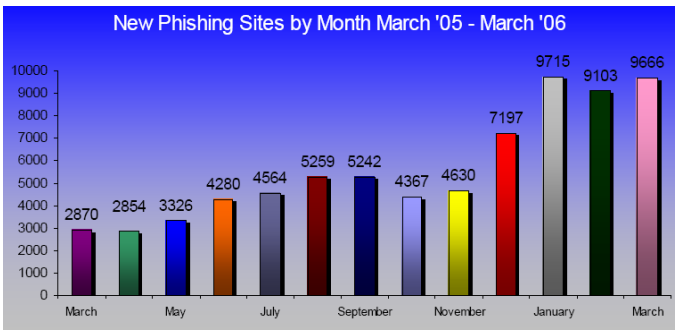
© 2006, Gary C. Kessler 

# Online Risks

- Phishing
- Malware
  - » Trojan horses, backdoors, rootkits, keyloggers
- Credential stealing attacks
- Channel breaking attacks
- Nigerian 419 and other scams

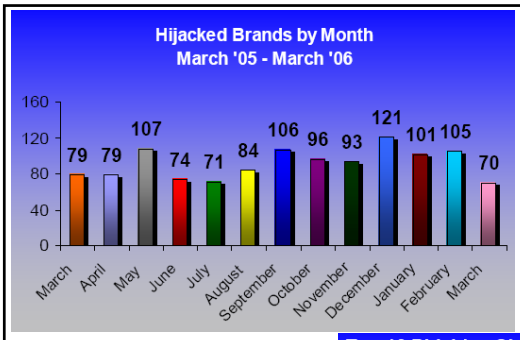
© 2006, Gary C. Kessler 

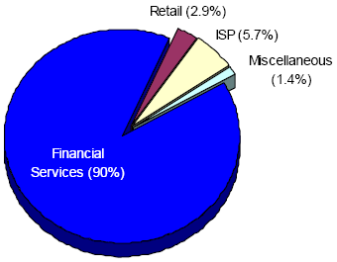



**From Anti-Phishing Working Group**

© 2006, Gary C. Kessler 

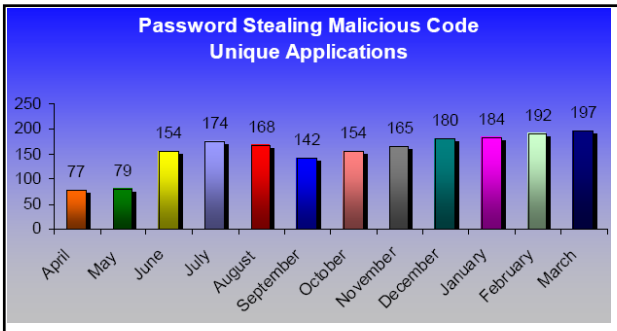


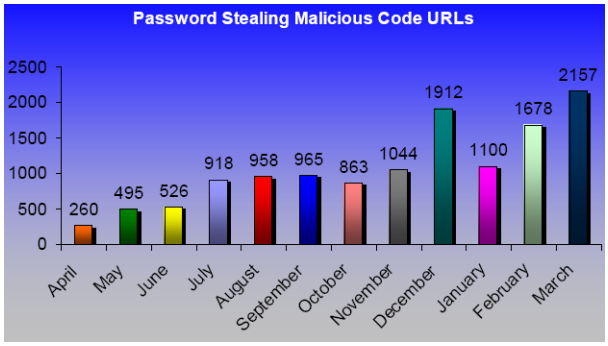



From Anti-Phishing Working Group

© 2006, Gary C. Kessler

8



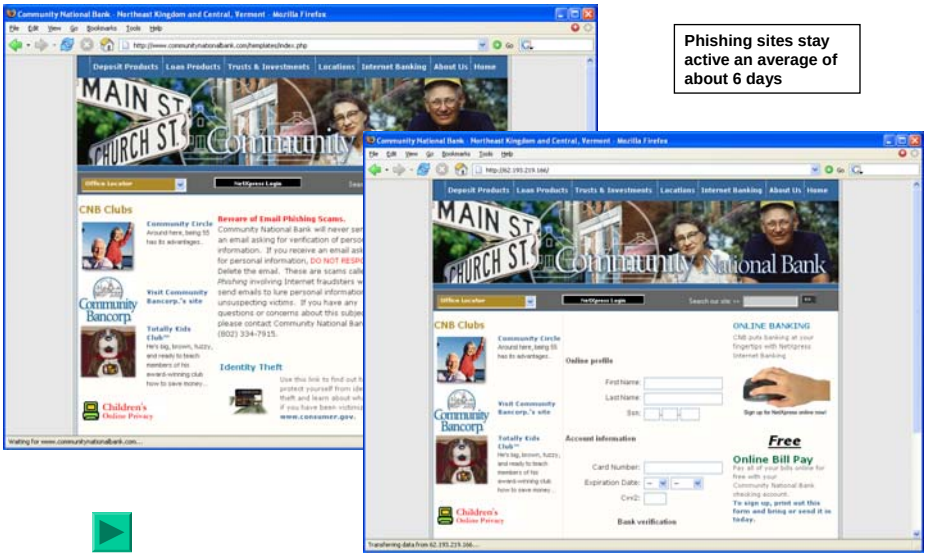




From Anti-Phishing Working Group

© 2006, Gary C. Kessler

9

# Phishing

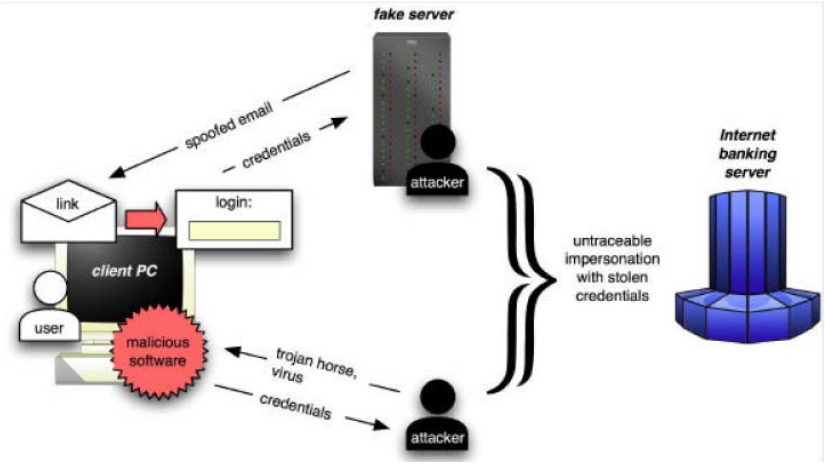



**Phishing sites stay active an average of about 6 days**



# DNS Cache Poisoning (Pharming)

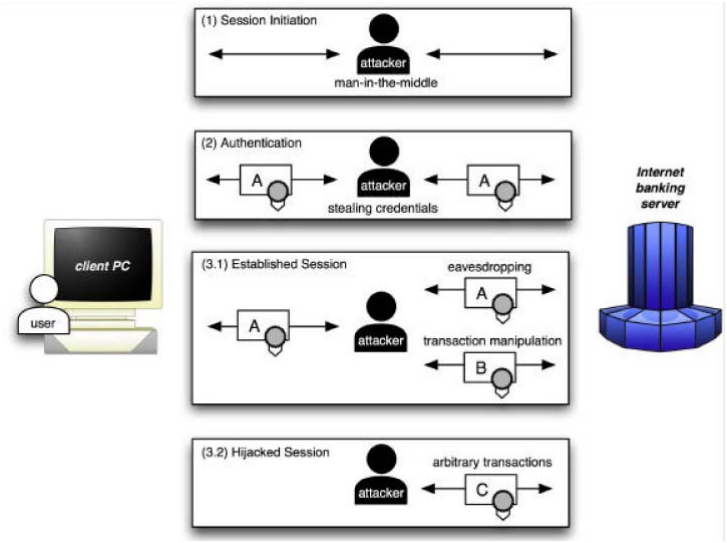
# Credential Stealing Attack Scenarios




From Hiltgen, et al., 2006



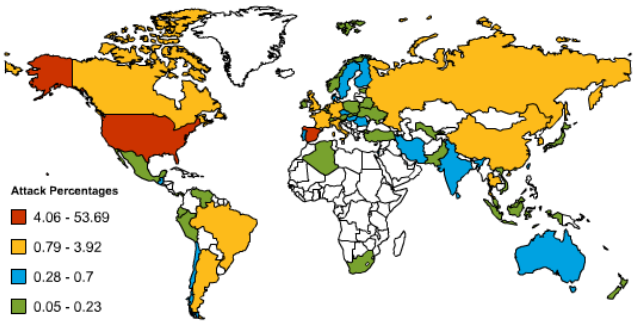
# Channel Breaking Attack Scenarios






From Hiltgen, et al., 2006

# Prevalence of the Problem




**"Phishing and Crimeware Map" from *http://www.antiphishing.org/crimeware.html*, 4/27/2006**

© 2006, Gary C. Kessler 

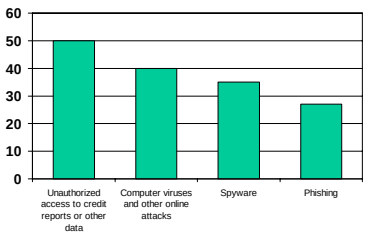
# Nigerian 419 Scams

- These scams has evolved from letters to faxes to e-mails
  - » Timely, using names that are in the news
  - » Believable...
    - To people with larceny in their hearts
- See *http://www.bustedupcowgirl.com/scampage.html*

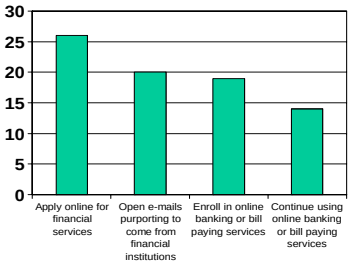
© 2006, Gary C. Kessler 

# Impact on Consumers

**Online banking customers are concerned that personal information will be compromised by (%):**




**Concerns about phishing have caused consumers not to (%):**




**RESULTS:**
- **Loss of consumer confidence**
- **A lingering question of "why"?**

**Source: Gartner Group**

© 2006, Gary C. Kessler



# Motivation of the Bad Guy

- The old fashioned way
  - » Small gain, great risk
  - » Victim can identify you
  - » Victim can fight back
  - » Police can chase you
  - » Gun enhancements
  - » Long prison terms

- Id. theft method
  - » High profit, low risk
  - » No victim contact
  - » No weapon use
  - » Police understaffed and overwhelmed
  - » Probation or misdemeanor -- **if** caught
  - » The loot is delivered!

© 2006, Gary C. Kessler

# FFIEC Guidance Overview

© 2006, Gary C. Kessler


# FFIEC Overview

- Federal Financial Institutions Examination Council comprises the following agencies:
  - » Board of Governors of the Federal Reserve System
  - » Federal Deposit Insurance Corporation
  - » National Credit Union Administration
  - » Office of the Comptroller of the Currency
  - » Office of Thrift Supervision
- Mission
  - » Formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions and to make recommendations to promote uniformity in the supervision of financial institutions
  - » Established March 1979

© 2006, Gary C. Kessler

# Information Technology Papers

- *Authentication in an Electronic Banking Environment* (August 2001)
- *Risk Management of Free and Open Source Software* (October 2004)
- *Authentication in an Internet Banking Environment* (October 2005)
  - » Supersedes 2001 *Guidance*

© 2006, Gary C. Kessler


# Information Security Topics

- Other FFIEC agency papers include:
  - » *FFIEC Information Security Handbook* (November 2003)
  - » *Guidance on Safeguarding Customers Against E-Mail and Internet Related Fraud* (March 2004)
  - » *Interagency Informational Brochure on Phishing Scams* (September 2004)
  - » *Putting an End to Account- Hijacking Identity Theft* (December 2004; June 2005)
  - » *Guidance on Mitigating Risks From Spyware* (July 2005)
  - » *Guidance on How Financial Institutions Can Protect Against Pharming Attacks* (July 2005)

© 2006, Gary C. Kessler

# FFIEC Guidance

- 2001 Guidance focus was risk management controls needed to authenticate e-banking customers
- Since 2001:
  - » More laws related to protection of customer information
    - E.g., Gramm-Leach-Bliley Act (1999), Financial Data Protection Act (2005), California Security Breach Information Act (2003)
  - » Increased incidence of fraud and identity theft
  - » Better authentication technologies

© 2006, Gary C. Kessler


# FFIEC Guidance Highlights

- Financial institutions offering Internet-based services should use effective methods to authenticate the identity of customers using those services.
- Single-factor authentication methodologies may not provide sufficient protection for Internet-based financial services.
- FFIEC agencies consider single-factor authentication, when used as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties.
- Risk assessments should provide the basis for determining an effective authentication strategy according to the risks associated with the various products and services available to on-line customers.
- Customer awareness and education should continue to be emphasized because they are effective deterrents to the on-line theft of assets and sensitive information.

- Compliance expected by end of 2006

**From FFIEC, 2005**

© 2006, Gary C. Kessler

# Focus of 2005 Guidance

- 2005 Guidance focus is on three areas:
  - » Risk assessment
  - » Reliable authentication
  - » Customer awareness

© 2006, Gary C. Kessler 

# Risk Assessment

- Financial institutions should implement an ongoing risk assessment process of their Internet banking systems
- Evaluation factors:
  - » Type of customer (e.g., retail or commercial)
  - » Customer transactional capabilities (e.g., bill payment, wire transfer, or loan origination)
  - » Sensitivity of customer information being communicated
  - » Ease of use
  - » Volume of transactions

© 2006, Gary C. Kessler 

# Risk Assessment (2)

- Authentication methods, in particular, should be reviewed
  - » Single-factors (e.g., passwords and PINs) are inadequate as the sole authentication method for high-risk transactions
- The risk assessment process should:
  - » Identify all transactions and levels of access associated with Internet-based customer products and services;
  - » Identify and assess the risk mitigation techniques, including authentication methodologies, employed for each transaction type and level of access; and
  - » Include the ability to gauge the effectiveness of risk mitigation techniques for current and changing risk factors for each transaction type and level of access.

© 2006, Gary C. Kessler 

# Reliable Authentication

- Authentication systems must be able to reliably verify the identity of the individual or organizational customer
  - » Account origination
    - Particular requirement of USA PATRIOT Act
  - » Customer verification
- Monitoring, auditing, and reporting capabilities must also be in place

© 2006, Gary C. Kessler 

## Customer Awareness

- User education is the **key** defense against fraud and identity theft
- Financial institutions are advised to implement a customer awareness program
- Periodically evaluate efficacy, using such criteria as:
  - » Number of customers reporting fraud attempts
  - » Number of clicks on institution's security links
  - » Amount of educational statement stuffers or mailings
  - » Monetary loss due to identity theft, fraud, etc.

© 2006, Gary C. Kessler 

## Authentication in Online Systems

© 2006, Gary C. Kessler 

## Authentication Factors

- All online authentication systems can be classified by the identifying factor(s) employed:
  - » Something you *know*
  - » Something you *have*
  - » Something you *are*
    - Includes something you *do*

© 2006, Gary C. Kessler 

## Passwords

- Most convenient (and common) form of protection
  - » What you know vs. what you have/are
- Weakest form of protection because people choose bad passwords
  - » Names, numbers, hobbies, username, ...
  - » ...and you only need a few bad ones to open your entire system

© 2006, Gary C. Kessler 

# Password Limitations

- Which would you prefer?
  - » 6-8 characters; at least one alpha and one numeric; no expiration
  - » 6-14 characters; at least one upper case, lower case, number, and special character; 90-day expiration
- Password guessing is successful up to 90% of the time

**Very Secure Passwords**

© 2006, Gary C. Kessler 

# The Efficacy of Passwords

***Time Required to Search All Possible Keys (at 2 million keys/sec) in a Brute Force attack***

| Characters | 4-octet | 5-octet | 6-octet | 7-octet | 8-octet |
|---|---|---|---|---|---|
| Lowercase letters (26) | 0.25 s | 6 s | 2.6 min | 1.1 hr | 1.2 day |
| Lowercase alphanumeric (36) | 0.85 s | 30 s | 18.4 min | 10.8 hr | 16.2 day |
| All alphanumeric (62) | 7.5 s | 7.5 min | 7.9 hr | 20.3 day | 3.5 yr |
| Printable (95) | 42 s | 63 min | 4.3 day | 1.1 yr | 104.5 yr |
| 7-bit ASCII (128) | 2.3 min | 4.7 hr | 25.5 day | 8.9 yr | 1,141.5 yr |
| 8-bit ASCII (256) | 36 min | 6.35 day | 4.5 yr | 1,141 yr | 285,388 yr |

**NOTE: A 1.2 GHz Pentium can perform 2M checks/sec.**

Adapted from *Applied Cryptography*

© 2006, Gary C. Kessler 

# "What You Have" Authentication

- Based upon some item in the possession of the user
  - » Tokens
  - » Dongles
  - » One-time Passwords

© 2006, Gary C. Kessler 

# "What You Are" Authentication

- Based upon some physical characteristic of the user
  - » *Biometrics*

**http://www.biometricsinstitute.org/products.html**

© 2006, Gary C. Kessler 

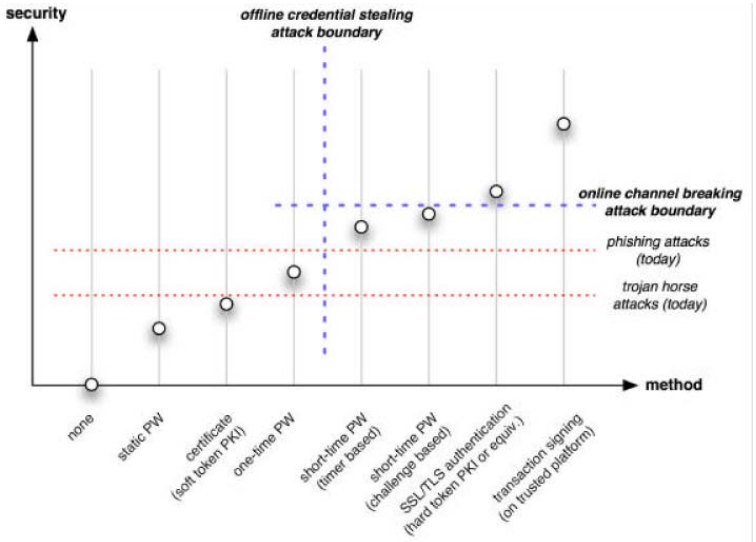
# Biometrics

- Iris/retina scan, fingerprints/handprints, voice prints, DNA, face recognition, lip movement, signature, click rate

- These technologies are good but not perfect nor foolproof
  - » "Gattica" -- gummy bears -- "Minority Report"

© 2006, Gary C. Kessler 

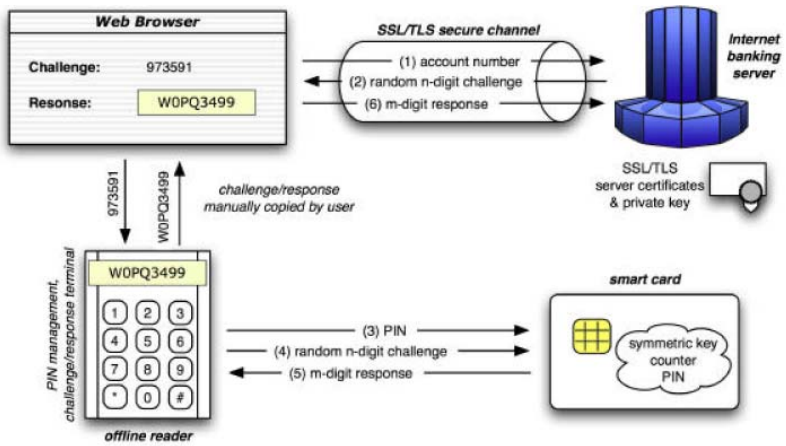
# Internet Banking Authentication Taxonomy




© 2006, Gary C. Kessler

From Hiltgen, et al., 2006

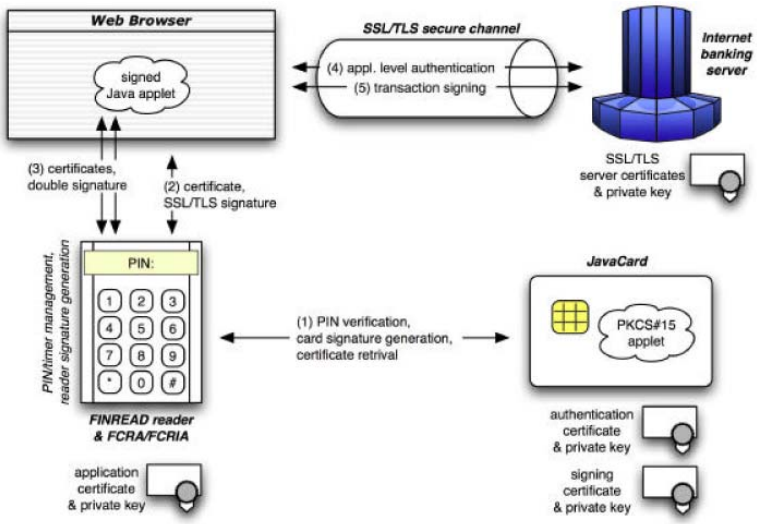
# Short-Time Password




From Hiltgen, et al., 2006

© 2006, Gary C. Kessler 

# Certificate-Based Solution




© 2006, Gary C. Kessler

From Hiltgen, et al. (2006)

# Online Authentication Models

- One-time password scratch card
- One-time password tokens

- Smart cards
  - » Requires reader (plus drivers, proper OS...)

- Out-of-Band (OOB) Authentication
  - » À la confirming telephone call to complete a financial transaction

© 2006, Gary C. Kessler 

# Online Authentication Models

- IP address and geo-location
  - » Compare IP host address to customer's known location
  - » Require additional authentication information if questionable location
- Mutual authentication
  - » Based upon public-key infrastructure
  - » Uses SSL so that client and server can exchange certificates

© 2006, Gary C. Kessler 

# Secure Computing

- SafeWord for *online*Banking
  - » Two-factor authentication
  - » SafeWord server integrates with bank's applications and databases
  - » OTP passwords via tokens or SMS messages

http://www.securecomputing.com/

© 2006, Gary C. Kessler



# Aladdin Knowledge Systems

- eToken PRO Smartcard
  - » Stores user's private keys, passwords, and certificates, using 1024- or 2048-bit RSA authentication and digital signatures
  - » Usable with any standard smart card reader
  - » Two-factor authentication requires smart card and password
  - » Provides strong authentication and non-repudiation for sensitive applications such as e-banking, e-commerce, and other financial transactions

http://aladdin.com/

© 2006, Gary C. Kessler

# RSA Security

- SecurID
  - » Family of products providing two-factor authentication, using AES and RSA
    - Key fob, card, PINpad and USB hardware
    - Software tokens available for Windows, Pocket PC, PalmOS, BlackBerry, and Ericsson, Nokia, and NTT DoCoMo cell phones

http://www.rsasecurity.com

© 2006, Gary C. Kessler


# PassMark Security

- Comprehensive solution to provide two-factor, two-way authentication with minimal inconvenience to end user
  - » Designed specifically to address FFIEC Guidance
  - » Provides mechanism for server to authenticate client and client to authenticate server
  - » Two factors are a PassMark image and user's computer's Device ID

http://www.passmarksecurity.com/

© 2006, Gary C. Kessler

# PassMark Authentication

- New users self-register, during which a unique Device ID is assigned to, and stored on, their access device (e.g., computer or PDA). Supplemental authentication methods include knowledge-based questions, and OOB email and phone confirmations
- When a user accesses the server from a known computer, authentication is instantly performed using PassMark image
- Self-registration is employed for each new device, allowing user to employ more than one computer

- PassMark server uses heuristics to determine if an access attempt is "suspicious," in which case additional authentication information is requested
- A *deviceprint* is also used to supplement the Device ID
  - » HTTP headers, OS registry, software configuration, IP address
  - » Aid in forensics and incident response

© 2006, Gary C. Kessler 

# Concluding Comments

© 2006, Gary C. Kessler 

## Is Cryptography the Answer?

- What problems are **really** solved with two-factor authentication?

"Whoever thinks his problem can be solved using cryptography, doesn't understand his problem and doesn't understand cryptography."

Attributed by Roger Needham and Butler Lampson to each other

© 2006, Gary C. Kessler


## What Problems Will be Solved?

- Two-factor authentication "solves the security problems we had ten years ago, not the security problems we have today" (Bruce Schneier)
  - » Two-factor authentication, particularly when employed with OOB methods, can be very effective but will not stop phishing, identity theft, and fraud
  - » When we thwart one attack vector, Bad Guys merely shift to another
- The lesson: Don't become complacent!

© 2006, Gary C. Kessler

## Two-Factor Authentication

- 2005 Guidance focuses on authentication as primary solution
  - » But does it *require* two-factor authentication???
- "Multifactor authentication, layered security or other controls reasonably calculated to mitigate those risks" (FFIEC, 2005, pg. 2)

© 2006, Gary C. Kessler 

## Customer Awareness Redux

- Customer awareness and education is often overlooked or downplayed....
- End users are **the** key to protecting systems
  - » Aware users don't give out or share their PINs, credit cards, tokens, etc.
- Smart users can save weak security but good security cannot save clueless users

© 2006, Gary C. Kessler 

# Summary

- Online banking: Features and risks
  - » Phishing demo
  - » DNS cache poisoning demo
- FFIEC Guidance Overview
- Authentication methods
  - » Two-factor authentication
  - » Options for online banking
- Is two-factor authentication the correct approach?

© 2006, Gary C. Kessler 

# References

Anti-Phishing Working Group. (2006, March). *Phishing activity trends report*. Retrieved April 20, 2006, from http://www.antiphishing.org/reports/apwg_report_mar_06.pdf

Federal Financial Institutions Examination Council (FFIEC). (2005, October 12). *Authentication in an Internet banking environment*. Financial Institution Letter, FIL-103-2005. Washington, D.C.: Federal Deposit Insurance Corp. (FDIC). Retrieved March 18, 2005, from http://www.ffiec.gov/pdf/authentication_guidance.pdf

Fox, S. (2005, February). *The state of online banking*. Pew Internet & American Life Project. Retrieved April 27, 2006, from http://www.pewinternet.org/pdfs/PIP_Online_Banking_2005.pdf

Hiltgen, A., Kramp, T., & Weigold, T. (2006, March/April). Secure Internet banking authentication. *IEEE Security & Privacy*, *4*(2), 21-29.

© 2006, Gary C. Kessler 

# Acronyms and Abbreviations

| | |
|---|---|
| **AES** | **Advanced Encryption Standard** |
| **ASCII** | **American Standard Code for Information Interchange** |
| **ATM** | **Automatic Teller Machine** |
| **DNA** | **Deoxyribonucleic acid** |
| **DNS** | **Domain Name System** |
| **FFIEC** | **Federal Financial Institutions Examination Council** |
| **HTTP** | **Hypertext Transport Protocol** |
| **IP** | **Internet Protocol** |
| **ISP** | **Internet Service Provider** |
| **OOB** | **Out-of-band** |
| **OS** | **Operating system** |
| **OTP** | **One-time password** |
| **PDA** | **Personal digital assistant** |
| **PIN** | **Personal Identity Number** |
| **PKCS** | **Public-Key Cryptography Standard** |
| **PKI** | **Public key infrastructure** |
| **PW** | **Password** |
| **RSA** | **Rivest, Shamir, and Adleman** |
| **SMS** | **Short Message Service** |
| **SSL** | **Secure Sockets Layer** |
| **TLS** | **Transport Layer Security** |
| **USB** | **Universal Serial Bus** |

© 2006, Gary C. Kessler 

# Author Contact Information

**Gary C. Kessler**
Computer & Digital Forensics program
Center for Digital Investigation
Champlain College
163 South Willard Street
Burlington, VT 05401

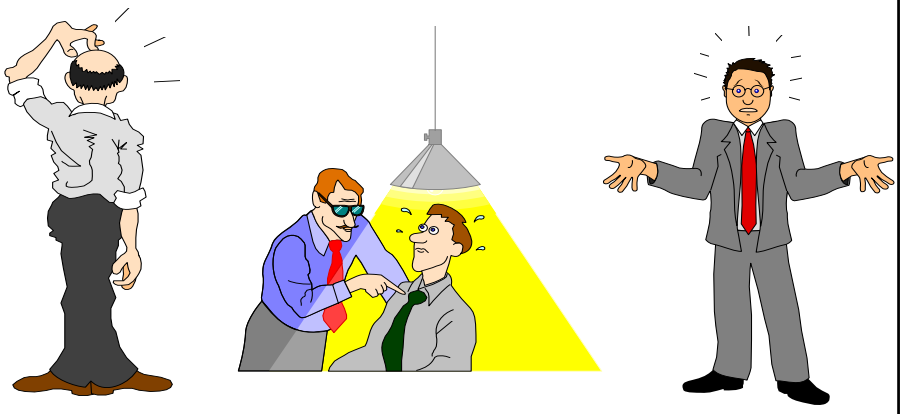
**office:** 802-865-6460
**cell:** 802-238-8913
**fax:** 802-865-6446 or 630-604-5529
**e-mail:** gary.*kessler@champlain.edu*
*kumquat@sover.net*

*http://digitalforensics.champlain.edu*
*http://c3di.champlain.edu*
*http://www.garykessler.net*

*The author preparing his presentations...*

© 2006, Gary C. Kessler 

# Questions? Comments? Queries?



© 2006, Gary C. Kessler