

SECURE
COMPUTING

**Session
G4**



28th Annual
Computer
Security
Conference

**Site-Specific Planning for
Authentication Systems**

Richard E. Smith, Ph.D., CISSP
rick_smith@securecomputing.com
28 October 2001

29 Oct 01 Session G4 - 28th CSI Annual Conference 1

SECURE
COMPUTING


Outline

- **Introduction**
- **Authentication Factors**
 - What you know
 - What you have
 - What you are
- **Authentication Design Patterns**
 - Direct pattern (uses traditional password files)
 - Indirect pattern (uses authentication server)
 - Off-Line pattern (uses public key certificates)

29 Oct 01 Session G4 - 28th CSI Annual Conference 2

SECURE
COMPUTING

Authentication



Cover art from
Authentication: From Passwords to Public Keys
by Richard E. Smith © 2002,
Addison Wesley.
Illustration by Peter Steiner,
The Cartoon Bank. Used by
permission.

*"On the Internet, no one
knows you're a dog."*

29 Oct 01 Session G4 - 28th CSI Annual Conference 3

SECURE
COMPUTING

Identity vs. Authentication

- **Identity Question: "Who Am I?"**
 - Mixed breed male dog, 36 dog-years old
- **Identity Question: "What is my name?"**
 - "Bowser"

Authentication ties a name to someone who is using a computer

- We tie details of identity, like permissions, to the user name
 - A different problem: "Access Control"
- Our measure of success: the computing system always associates a user name with its legitimate owner

29 Oct 01 Session G4 - 28th CSI Annual Conference 4

SECURE COMPUTING

The Problem: Masquerade

| <u>Attacks</u> | | <u>Defenses</u> |
|-------------------------|---|------------------------|
| ?? | ← | One-Time Passwords |
| Network Sniffing | ← | Password Tokens |
| Password Sharing | ← | Memory Protection |
| Keystroke Sniffing | ← | Help Desk Restrictions |
| Social Engineering | ← | Guess Detection |
| Guessing | ← | Password Hashing |
| Steal the Password File | ← | Passwords |

29 Oct 01 Session G4 - 28th CSI Annual Conference 5

SECURE COMPUTING

Sniffing Attacks

1. Cathy logs on with her password
User: croe
Password: egg

2. Attacker sniffs the network traffic

3. Cathy's server logs her on
*User croe logged on at 1:00

4. Later, the attacker logs on as Cathy
User: croe
Password: egg
*User croe logged on at 7:00

From Authentication © 2002. Used by permission.

29 Oct 01 Session G4 - 28th CSI Annual Conference 6

Brute Force Attacks

- **Off-Line Attacks**
 - Example - "Dictionary Attack"
 - Uses intercepted information about users' passwords
 - Most powerful attack - fast and hard to detect
- **Interactive Attacks**
 - Example: PIN guessing attacks
 - Trial-and-error attempt to use a server
 - Limited to server's speed, and failures can be detected
- **Team Attacks**
 - Team of people take turns trying the masquerade
 - Limited to server's speed, and failures can be detected

29 Oct 01

Session G4 - 28th CSI Annual Conference

7

The Lessons

- There are no perfect security systems
- It makes no sense to spend a fortune on security if the potential damage is limited
- It makes no sense to scrimp on security if the potential for damage is large
- Many security risks are site-specific
 - Attackers don't work as hard if there's no payoff
 - Insiders have different motivations than outsiders
 - Different techniques work best with different people
- Tailor your authentication to your site

29 Oct 01

Session G4 - 28th CSI Annual Conference

8

What guides our choices?

- **Who and where are the users?**
 - Inside the enterprise's offices, outside, or both?
 - People with established relationships or anonymous?
- **How big is your operation?**
 - Do you have one or two servers, or several, or hundreds?
- **Where is the computing equipment?**
 - Does everyone use your equipment to access your computers?
 - Do authorized users connect remotely?
- **What do you have to lose?**
 - Merchandise? Subscription payments? Deposits?
- **How much can you afford to spend?**

What are our choices?

- **How users prove their identities**
 - Passwords vs. tokens vs. biometrics, or combinations thereof - Authentication Factors
 - Remote and mobile users may face special risks and portability issues
- **How we manage user records - reflects "design patterns" for authentication**
 - Traditional per-host databases ("direct")
 - Shared authentication servers ("indirect")
 - Public key certificates ("off-line")

SECURE
COMPUTING

Passwords: Things you know

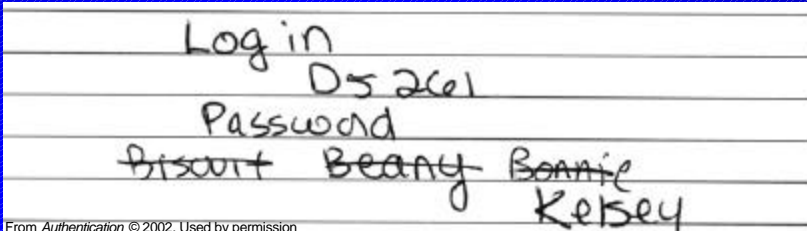
| <u>Benefits</u> | <u>Problems</u> |
|---------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> • Cheap to implement • Easy to share • Portable | <ul style="list-style-type: none"> • Sniffing attacks • Easy to share • Can't detect if they were sniffed or shared • Passwords are either easy to guess or hard to remember • Administrative costs of forgotten passwords |

29 Oct 01 Session G4 - 28th CSI Annual Conference 11

SECURE
COMPUTING

Passwords in Practice

- The Rule for Strong Passwords:
The password must be impossible to memorize and never written down
- The Result of this Rule
 - look under some mouse pads and find ---



From *Authentication* © 2002. Used by permission

29 Oct 01 Session G4 - 28th CSI Annual Conference 12

Password Strength

- **Resisting a brute force guessing attack**
 - Estimate the average number of attempts required to succeed
 - Attacker makes a list of possible passwords and tries them all
 - # passwords in the list
 - % chance that someone chooses from that list
 - How many attempts to achieve 50-50 chance of success
 - Call this the Average Attack Space - represented by 2^x
- **An Ideal Example**
 - People choose completely random strings of characters
 - 96 characters to choose from, 8 characters long
 - 96^8 presents an average attack space of about 2^{45}

Weak in Practice

| Example | Type of Attack | Average Attack Space |
|-----------------------------|----------------|----------------------|
| Random 8-character password | Interactive | 2^{45} |
| Dictionary Attack | Off-Line | 2^{15} to 2^{23} |
| Mouse Pad Search | Interactive | 2^1 to 2^4 |

Passwords: When and When Not

When to Use

- Places where physical attacks are easier (internal use)
- Places where sniffing won't work (encryption)
- Places where guessing attacks can be detected

When NOT to Use

- Places where sniffing is practical (usually the Internet)
- Places where dictionary attacks are practical (usually the Internet)

Internet Password Safety

- **Not safe - plaintext protocols**
 - POP, IMAP, Telnet, HTTP
 - Attackers can sniff passwords directly without detection
- **A little safer - challenge response protocols**
 - Windows NTLM, MS-CHAP, Windows 2000, Kerberos
 - Attackers can intercept enough information for Off-Line Attack
 - Simple passwords are vulnerable
- **A lot safer - encryption protocols**
 - SSL for Web and Telnet, IPSEC for everything else
 - Attackers are reduced to interactive password guessing
 - Attacks on simple passwords can be detected

Authentication Tokens



From Authentication © 2002. Used by permission

- There are also “soft” tokens
 - Most tokens also provided in software implementations
 - “Public key” products often handle the private key with software-only mechanisms

29 Oct 01

Session G4 - 28th CSI Annual Conference

17

Tokens: Things you have

Benefits

- Hard to attack - uses a stronger secret than you get in a typical password
- Hard to forge - must often hack the hardware
- Hard to share - usually stored in hardware

Problems

- Expensive - must buy hardware and/or special authentication software
- Can be lost or stolen
- Risk of hardware failure
- Not always portable

29 Oct 01

Session G4 - 28th CSI Annual Conference

18

SECURE COMPUTING

Hardware Tokens

From Authentication © 2002. Used by permission

- Resist copying and other attacks by storing the secret in a tamper-resistant package.

29 Oct 01 Session G4 - 28th CSI Annual Conference 19

SECURE COMPUTING

One-Time Password Tokens

1. Cathy uses her token to get the next one-time password

2. Cathy logs on with the one-time password

3. Attacker "sniffs" the network traffic

4. Cathy's server logs her on

User: croe
Password: ff7e6c

*User croe logged on at 1:00

From Authentication © 2002. Used by permission

Attacker can't reuse the sniffed password

29 Oct 01 Session G4 - 28th CSI Annual Conference 20

SECURE COMPUTING


Tokens Resist Attacks

| Example | Type of Attack | Average Attack Space |
|----------------------------|----------------|-----------------------|
| Passw ord | Off-Line | 2^{15} to 2^{23} |
| One-Time Password Token | Interactive | 2^{19} to 2^{23} |
| One-Time Password Token | Off-Line | 2^{54} to 2^{63} |
| Smart Card with Public Key | Off-Line | 2^{63} to 2^{116} |

29 Oct 01
Session G4 - 28th CSI Annual Conference
21

SECURE COMPUTING

Biometrics: Things you are



From *Authentication* © 2002. Used by permission

Recognizes a user's physical characteristics

29 Oct 01
Session G4 - 28th CSI Annual Conference
22

SECURE
COMPUTING

Biometrics: Things you are

| | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <h3><u>Benefits</u></h3> <ul style="list-style-type: none">• Easiest to use | <h3><u>More Problems</u></h3> <ul style="list-style-type: none">• Privacy risks for users• Characteristic can't be changed if it's been intercepted• Reliability - doesn't always recognize legitimate users• Characteristic can be injured |
| <h3><u>Problems</u></h3> <ul style="list-style-type: none">• Often expensive - usually requires special biometric readers• Attackers can sniff and replay a biometric reading on a network | |

29 Oct 01 Session G4 - 28th CSI Annual Conference 23

SECURE
COMPUTING

Multi-Factor Authentication

- We cover the weaknesses of individual techniques (tokens, passwords, biometrics) by combining two or more in one mechanism
- Two Factor Authentication
 - ATM Cards - card plus PIN
 - One-time password token with a keypad - token plus PIN
 - Biometric reading protected with a secret encryption key
- Three Factor Authentication
 - Token + memorized PIN + biometric reading
 - Rarely used

29 Oct 01 Session G4 - 28th CSI Annual Conference 24

SECURE
COMPUTING

Multi-Factor Token

From Authentication © 2002. Used by permission.

Fingerprint “unlocks” the authentication token

29 Oct 01

Session G4 - 28th CSI Annual Conference

25

SECURE
COMPUTING

Summary: Factors

- **Passwords are still the cheapest and most common**
 - Can not protect valuable assets - too easy to attack
 - Risky on the Internet unless you use encryption, too
- **Biometrics have limited use on networks**
 - Too easy to intercept and replay
 - Must be used in conjunction with cryptography
- **Tokens (hard or soft) give strongest protection**
 - Embedded cryptographic secrets can be hard to attack
 - Hardware tokens prevent sharing and delegation
 - Tokens must have PINs to protect against theft

29 Oct 01

Session G4 - 28th CSI Annual Conference

26

Design Patterns

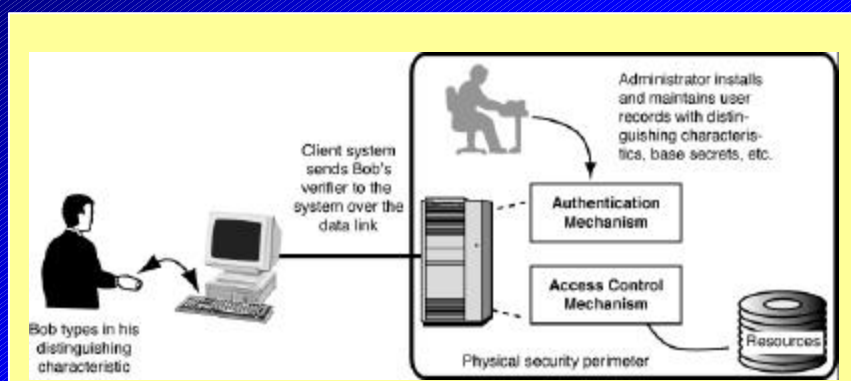
- **Local Pattern** - not discussed - rarely relevant
 - Example: isolated laptops and workstations
- **Remote Access: “Direct” and “Indirect”**
- **Direct Pattern**
 - Classic single-host servers: LANMAN, NetWare 3, Unix V7
- **Indirect Pattern**
 - Modern systems using authentication servers
 - Examples: RADIUS, Kerberos, Windows NT and 2K, TACACS
- **Off-Line Pattern**
 - Systems that validate public key credentials without a server

29 Oct 01

Session G4 - 28th CSI Annual Conference

27

Direct Authentication



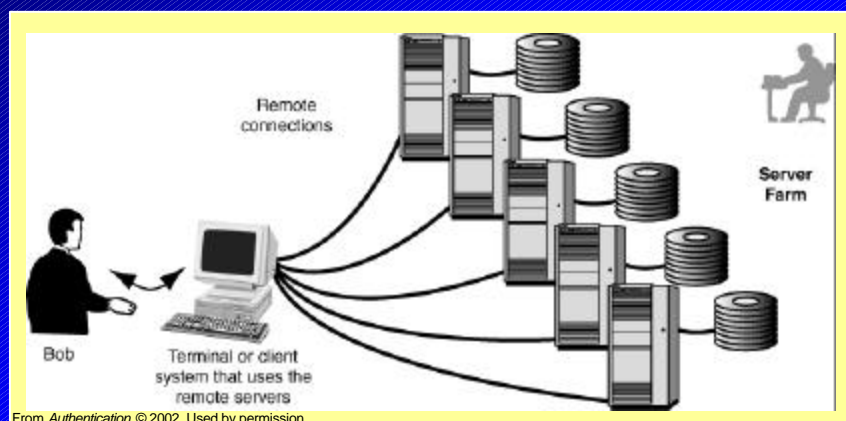
- Threat of sniffing on the data link
- OK for small sites; impractical for larger ones

29 Oct 01

Session G4 - 28th CSI Annual Conference

28

Server Farm Dilemma



A single sign-on problem - how can we easily let Bob connect to any or all servers?

29 Oct 01

Session G4 - 28th CSI Annual Conference

29

Direct Administration: Behavior in Practice

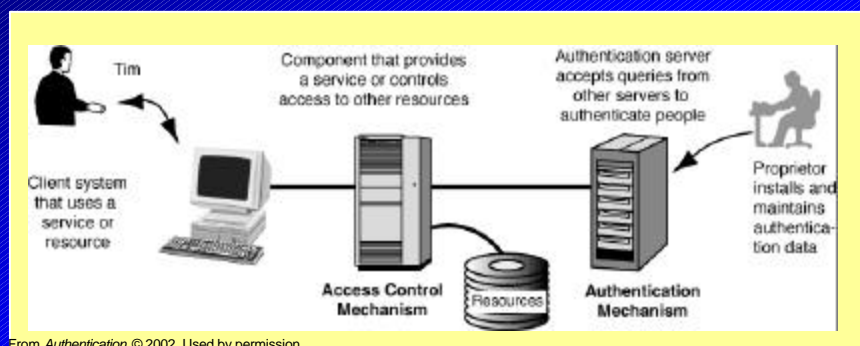
- **Single point of service (one server)**
 - Add User - Easy -
 - Just update the server's user records
 - Change takes effect immediately
 - Revoke User - Easy - works the same as adding users
- **Multiple points of service (many servers)**
 - Add User - Hard - must update each server individually
 - Revoke User - Hard - must update each server individually
- **Multiple Enterprises (servers owned by others)**
 - Add User - Hard - same as for multiple points of service (above)
 - Revoke User - Hard - same as for multiple points of service

29 Oct 01

Session G4 - 28th CSI Annual Conference

30

Indirect Authentication



From Authentication © 2002. Used by permission

- Move authentication to separate, central server
- Application servers are authentication *agents*
- Authentication server shared among agents

29 Oct 01

Session G4 - 28th CSI Annual Conference

31

Indirect System Examples

- Traditionally Password Based
 - Kerberos, Windows NT, Windows 2000
 - Kerberos and Win2K may also support smart cards
- Traditionally Token Based
 - One-time password server products
 - Protocols: RADIUS, TACACS+, proprietary, Windows interop
 - Modern versions will also support smart cards
 - Secure Computing's SafeWord Server, RSA's ACE Server
 - Generic authentication support (passwords, biometrics)
 - SafeWord Server

29 Oct 01

Session G4 - 28th CSI Annual Conference

32

Indirect Security Issues

- **Sniffing or Attacks on Client traffic**
 - Same as for Direct pattern
 - Mostly a problem in larger sites, or with Internet links
 - Solve with one-time password technology
- **Sniffing or Attacks on Agent traffic**
 - Solved by using a state-of-the-art authentication protocol
 - Moderate strength: Kerberos, Windows NT, Windows 2K
 - Higher strength: RADIUS
- **Authentication Server Reliability**
 - Need server replication
 - Standard in Windows 2000, SafeWord

29 Oct 01

Session G4 - 28th CSI Annual Conference

33

Indirect Administration: Behavior in Practice

- **Single point of service (one server)**
 - Add User - Easy - same as for many servers
 - Revoke User - Easy - same as for many servers
- **Multiple points of service (many servers)**
 - Add User - Easy
 - Update the authentication server's records
 - Change takes effect immediately for all servers that use it
 - Revoke User - Easy - same as for adding users
- **Multiple Enterprises (servers owned by others)**
 - Add User - Hard or Easy - depends on relationship with others
 - Revoke User - Hard - must contact other enterprises

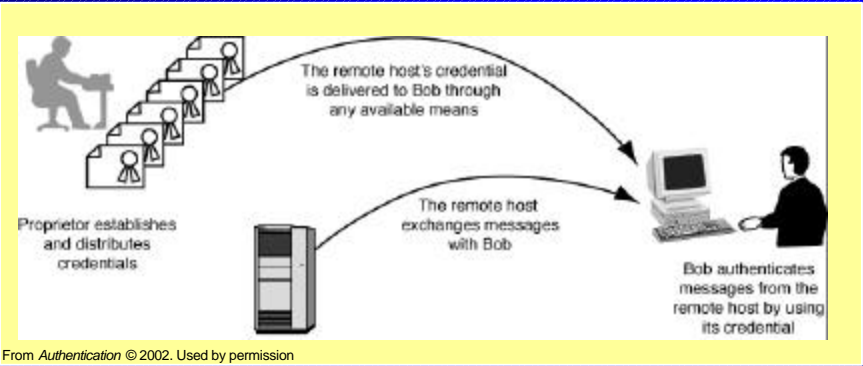
29 Oct 01

Session G4 - 28th CSI Annual Conference

34

SECURE COMPUTING

Off-Line Authentication



The diagram illustrates the off-line authentication process. On the left, a person is shown at a computer, with a stack of certificates below them. A text box says: "Proprietor establishes and distributes credentials". An arrow points from this stack to a server icon in the center. A text box above the arrow says: "The remote host's credential is delivered to Bob through any available means". From the server, an arrow points to a person at a computer on the right. A text box above this arrow says: "The remote host exchanges messages with Bob". Below the person at the computer, a text box says: "Bob authenticates messages from the remote host by using its credential".

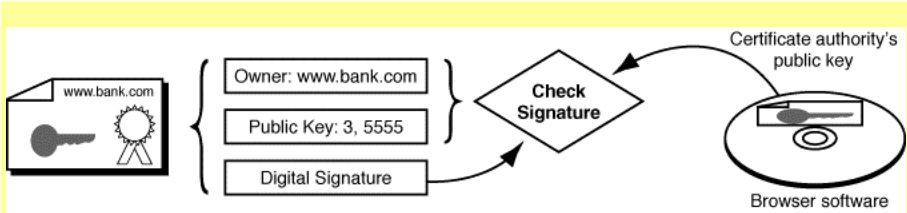
From *Authentication* © 2002. Used by permission

- Used by peoples' browsers to verify servers
- Checks credentials off-line
- Uses public key cryptography

29 Oct 01 Session G4 - 28th CSI Annual Conference 35

SECURE COMPUTING

Public Key Authentication



The diagram shows the public key authentication process. On the left, a certificate is shown with a key icon and a ribbon seal, labeled "www.bank.com". To its right, a bracket groups three items: "Owner: www.bank.com", "Public Key: 3, 5555", and "Digital Signature". An arrow points from this group to a diamond-shaped box labeled "Check Signature". To the right of the "Check Signature" box is a CD-ROM icon labeled "Browser software". An arrow points from the "Browser software" to the "Check Signature" box, with the label "Certificate authority's public key" above it.

From *Authentication* © 2002. Used by permission

1. The software uses a public key *embedded* in its code
2. The *embedded* public key verifies the certificate it receives that contains the *bank's* public key
3. The *bank's* public key stored in the certificate then *verifies* data received from that bank
4. We *authenticate* the bank by *verifying* the data

29 Oct 01 Session G4 - 28th CSI Annual Conference 36

Off-Line Security Issues

- **Integrity of Public Keys**
 - Verify the key by verifying its certificate
 - Verify the certificate using an authority's public key
 - Where do we get a public key to trust?
- **Integrity of Certificate Authorities**
 - Trickery can occasionally succeed
 - Attacking Microsoft thru Verisign (Microsoft bulletin MS01-017)
- **Mathematical Attacks on Public Keys**
 - Resist brute force cracking with large keys
 - Resist other attacks by using established standards
 - Public Key Cryptography Standards (PKCS)

29 Oct 01

Session G4 - 28th CSI Annual Conference

37

Off-Line Administration: Behavior in Practice

- **Single point of service (one server)**
 - Add User - Easy - same as for multiple enterprises
 - Revoke User - Hard - same as for multiple enterprises
- **Multiple points of service (many servers)**
 - Add User - Easy - same as for multiple enterprises
 - Revoke User - Hard - same as for multiple enterprises
- **Multiple Enterprises (servers owned by others)**
 - Add User - Easy - create and distribute user's certificate
 - Revoke User - Hard
 - Can't track down and update individual certificates
 - Must warn people not to use the user's revoked certificate

29 Oct 01

Session G4 - 28th CSI Annual Conference

38

Summary: Design Patterns

- **For most server applications: *Indirect* Pattern**
 - Network server examples: NTLM, Windows 2K, NetWare 4
 - Authentication servers: SafeWord, RSA Ace/Server
 - Protocols: RADIUS, TACACS, Kerberos
 - Scales well as servers proliferate
 - For reliability, choose a system with server replication
- **For multi-enterprise uses: *Off-Line* Pattern**
 - Examples: all public key infrastructure products
 - Interoperates with many *Indirect* server products
 - Lets less trustworthy devices perform reliable authentication
 - Delegates user enrollment
 - Problem: it's hard to revoke a user's credentials

29 Oct 01

Session G4 - 28th CSI Annual Conference

39

For Further Information

- Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, Wiley, 2001.
- Feghhi, Feghhi, and Williams, *Digital Certificates: Applied Internet Security*, Addison-Wesley, 1999.
- Jain, Bolle, and Pankanti, *Biometrics: Personal Identification in Networked Society*, Kluwer, 1999.
- Kaufman, Perlman, and Speciner, *Network Security: PRIVATE Communication in a PUBLIC World*, Prentice-Hall, 1995.
- Smith, *Authentication: From Passwords to Public Keys*, Addison-Wesley 2002. <http://www.visi.com/crypto/>

29 Oct 01

Session G4 - 28th CSI Annual Conference

40