Selling Security: Responding to market forces

Michael Spertus
Distinguished Engineer
Symantec Research Labs

Impacting Businesses

Increased Volume and Variety of Attacks is Increasing Liability

2005 Reported Data Breaches

15-Feb-05	ChoicePoint	ID thieves accessed	145,000
25-Feb-05	Bank of America	Lost backup tape	1,200,000
25-Feb-05	PayMaxx	Accidental exposure	25,000
8-Mar-05	DSW/Retail Ventures	Hacking	100,000
10-Mar-05	LexisNexis	Passwords compromised	32,000
11-Mar-05	Univ. of CA, Berkeley	Stolen laptop	98,400
11-Mar-05	Boston College	Hacking	120,000
12-Mar-05	NV Dept. of Motor Vehicle	Stolen computer	8,900
20-Mar-05	Northwestern Univ.	Hacking	21,000
20-Mar-05	Univ. of NV., Las Vegas	Hacking	5,000
22-Mar-05	Calif. State Univ., Chico	Hacking	59,000
23-Mar-05	Univ. of [illegible]	Hacking	7,000
28-Mar-05	Univ. of Chicago Hospital	Dishonest insider	unknown
1-Apr-05	Georgia DMV	Dishonest insider	"hundreds of th
5-Apr-05	MCI	Stolen laptop	16,500
8-Apr-05	Eastern National	Hacker	15,000
8-Apr-05	San Jose Med. Group	Stolen computer	185,000
11-Apr-05	Tufts University	Hacking	106,000
12-Apr-05	LexisNexis	Passwords compromised	Additional 280,0
14-Apr-05	Polo Ralph Lauren/HSBC	Hacking	180,000
14-Apr-05	Calif. Fastrack	Dishonest Insider	7,800
15-Apr-05	CA Dept. of Health Services	Stolen laptop	21,600
18-Apr-05	DSW/ Retail Ventures	Hacking	Additional 1,30
20-Apr-05	Ameritrade	Lost backup tape	200,000
21-Apr-05	Carnegie Mellon Univ.	Hacking	19,000
26-Apr-05	Mich. State Univ's Wharton C	Hacking	40,000
26-Apr-05	Christus St. Joseph's Hospital	Stolen computer	19,000
28-Apr-05	Georgia Southern Univ.	Hacking	20,000
28-Apr-05	Wachovia, Bank of America, F	Dishonest insiders	676,000
29-Apr-05	Oklahoma State Univ.	Missing laptop	37,000
2-May-05	Time Warner	Lost backup tapes	600,000
4-May-05	CO. Health Dept.	Stolen laptop	1,600
5-May-05	Purdue Univ.	Hacking	11,360
7-May-05	Dept. of Justice	Stolen laptop 80,000	80,000
11-May-05	Stanford Univ.	Hacking	9,900
12-May-05	Hinsdale Central High School	Hacking	2,400
16-May-05	Montebello, Calif.	Dishonest insider	7
18-May-05	Jackson Comm. College, Mich	Hacking	8,000
18-May-05	Univ. of Iowa	Hacking	30,000
19-May-05	Valdosta State Univ., GA	Hacking	40,000
20-May-05	Purdue Univ.	Hacking	11,000
26-May-05	Duke Univ.	Hacking	5,500
27-May-05	Cleveland State Univ.	Stolen laptop	44,420
28-May-05	Merlin Data Services	Bogus acct. set up	9,000
30-May-05	Motorola	Computers stolen	Not disclosed
5-Jun-05	CitiFinancial	Lost backup tapes	3,900,000
10-May-05	Fed. Deposit Insurance Corp. (	Not disclosed	6,000
16-Jun-05	CardSystems	Hacking	40,000,000
17-Jun-05	Kent State Univ.	Stolen laptop	1,400
18-Jun-05	Univ. of Hawaii	Dishonest Insider	150,000
22-May-05	Eastman Kodak	Stolen laptop	5,800
22-Jun-05	East Carolina Univ.	Hacking	250
25-May-05	Univ. of CT (UCONN)	Hacking	72,000
28-May-05	Lucas Cty. Children Services (	Accidental exposure	900
29-Jun-05	Bank of America	Stolen laptop	18,000
30-Jun-05	Ohio State Univ. Med. Ctr.	Stolen laptop	15,000
1-Jul-05	Univ. of CA, San Diego	Hacking	3,300
6-Jul-05	City National Bank	Lost backup tapes	Not disclosed
6-Jul-05	Mich. State Univ.	Hacking	27,000
19-Jul-05	Univ. of Southern Calif. (USC)	Hacking	270,000
[illegible]	[illegible] of Colorado-Boulder	Hacking	42,000
[illegible]	San Diego Employees Ret	Hacking	33,000
30-Jul-05	Calif. State Univ., Dominguez H	Hacking	9,613
31-Jul-05	Cal Poly Pomona	Hacking	31,077
2-Aug-05	Univ. of Colorado	Hacking	36,000
8-Aug-05	Sonoma State Univ.	Hacking	61,709
10-Aug-05	Univ. of North Texas	Hacking	39,000
17-Aug-05	Calif. State University, Stanisla	Hacking	900
18-Aug-05	Univ. of Colorado	Hacking	49,000
22-Aug-05	Air Force	Hacking	33,300
23-Aug-05	Univ. of [illegible] Hospital	Stolen laptop	3,851
30-Aug-05	J.P. Morgan, Dallas	Stolen Laptop	Not disclosed
30-Aug-05	Calif. State University, Chance	Hacking	154
10-Sep-05	Kent State Univ.	Stolen Computers	100,000
15-Sep-05	Miami Univ.	Accidental exposure	21,762
16-Sep-05	ChoicePoint	Hacking	9,903
19-Sep-05	Children's Health Council, San	Stolen backup tape	5,000
22-Sep-05	City University of New York	Exposed online	350
23-Sep-05	Bank of America	Stolen laptop	Not disclosed
23-Sep-05	LexisNexis Data Breaches	Dishonest insiders	310,000+
29-Sep-05	Univ. of Georgia	Hacking, at least	1,600
15-Oct-05	Montclair State Univ.	Exposed online	9,100

Hacking … 48%

Dishonest insider … 10%

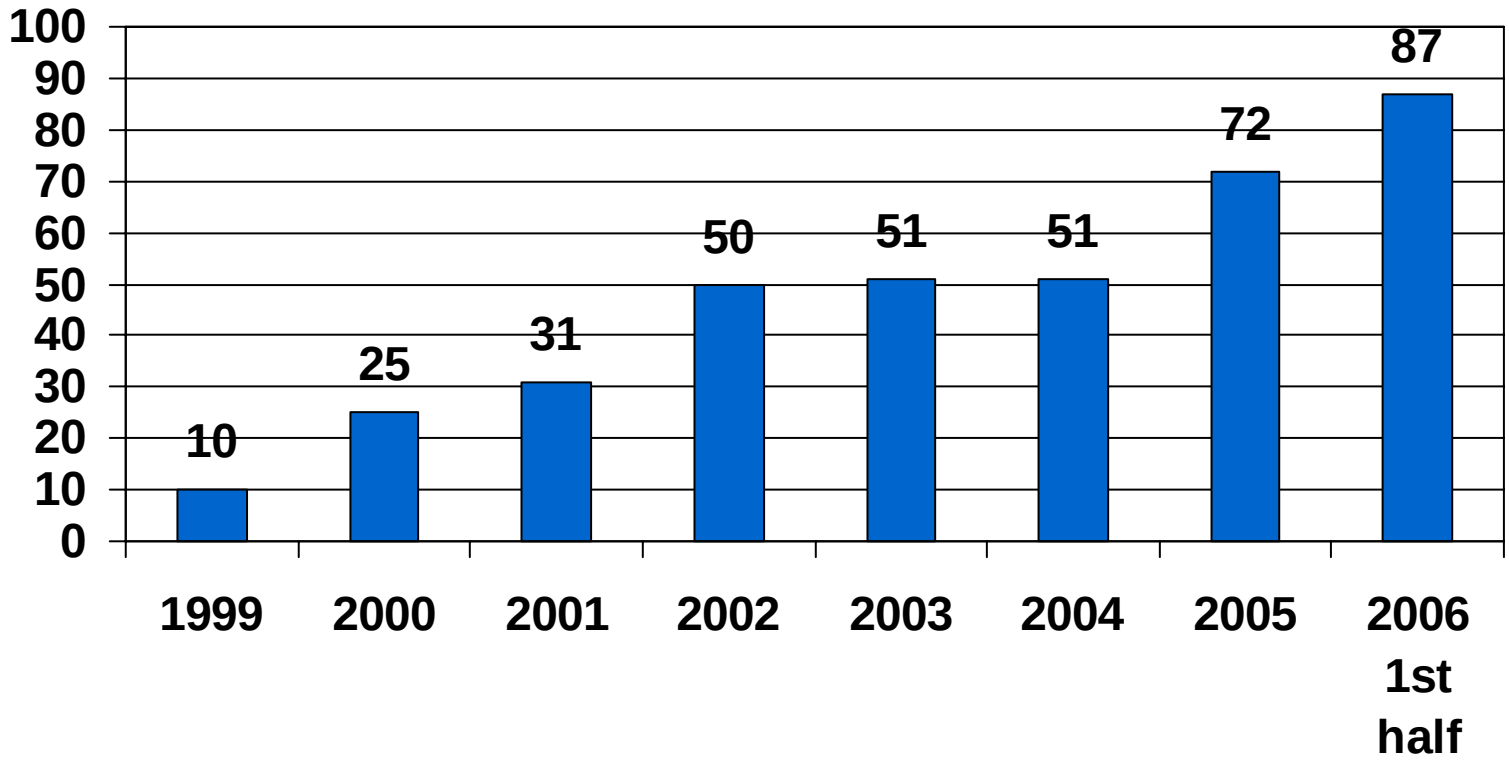
Accidental exposure … 15%

Stolen computers … 27%

130 reported breaches, 57+ million records affected!

Software Vulnerabilities (average discovered each week)

- 3 days average before exploit is available (80% easy to exploit)
- 97% of vulnerabilities rated moderate to severe

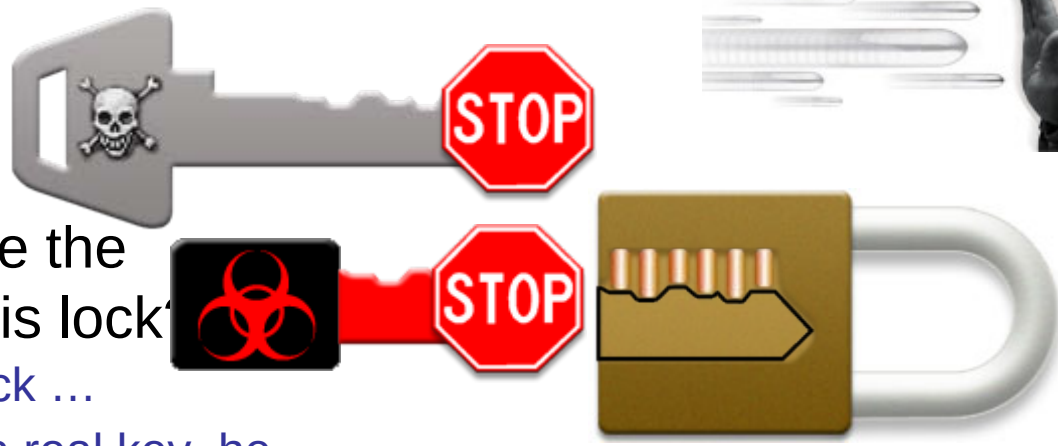


Source: Symantec Corporation, Internet Security Threat Report X September 25, 2006

Inflection Points

- Malware becomes self-spreading
- Protecting the system to protecting the transaction
  - “Is this malware?” becomes “Is this data safe”
- Separation of payload from delivery
- 15 minutes of fame to economic gain
- General threats to personalized threats
- Future: Malware outnumbers good software
  - The future is now for email
  - Blacklists replaced by whitelists
- Mobile devices become too powerful and general to lock down
- Reputation-based approaches
- Perimeter vs. endpoint
- Signatures switch from malware to vulnerabilities

Lock and Key



How could a guard determine the shape of a key that opens this lock?

Well, the guard could x-ray the lock …

So even though he's never seen a real key, he can tell me the shape of a key that can open this lock…

And from the pins, he could guess what shape key would open the lock…

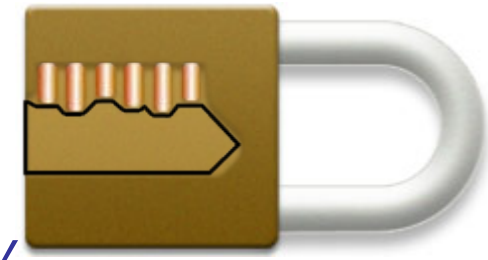
Given this specification, a guard could block anyone with a matching key from approaching the lock.

What if someone changes the shape of the key shaft to avoid detection?

We'll no longer recognize the key… But on the other hand, now it won't open the lock!

And it doesn't matter what color the key is, or what it's "head" looks like, all the guard cares about is the shape of the *key shaft*…

Lock and Key



A software vulnerability is just like our padlock.

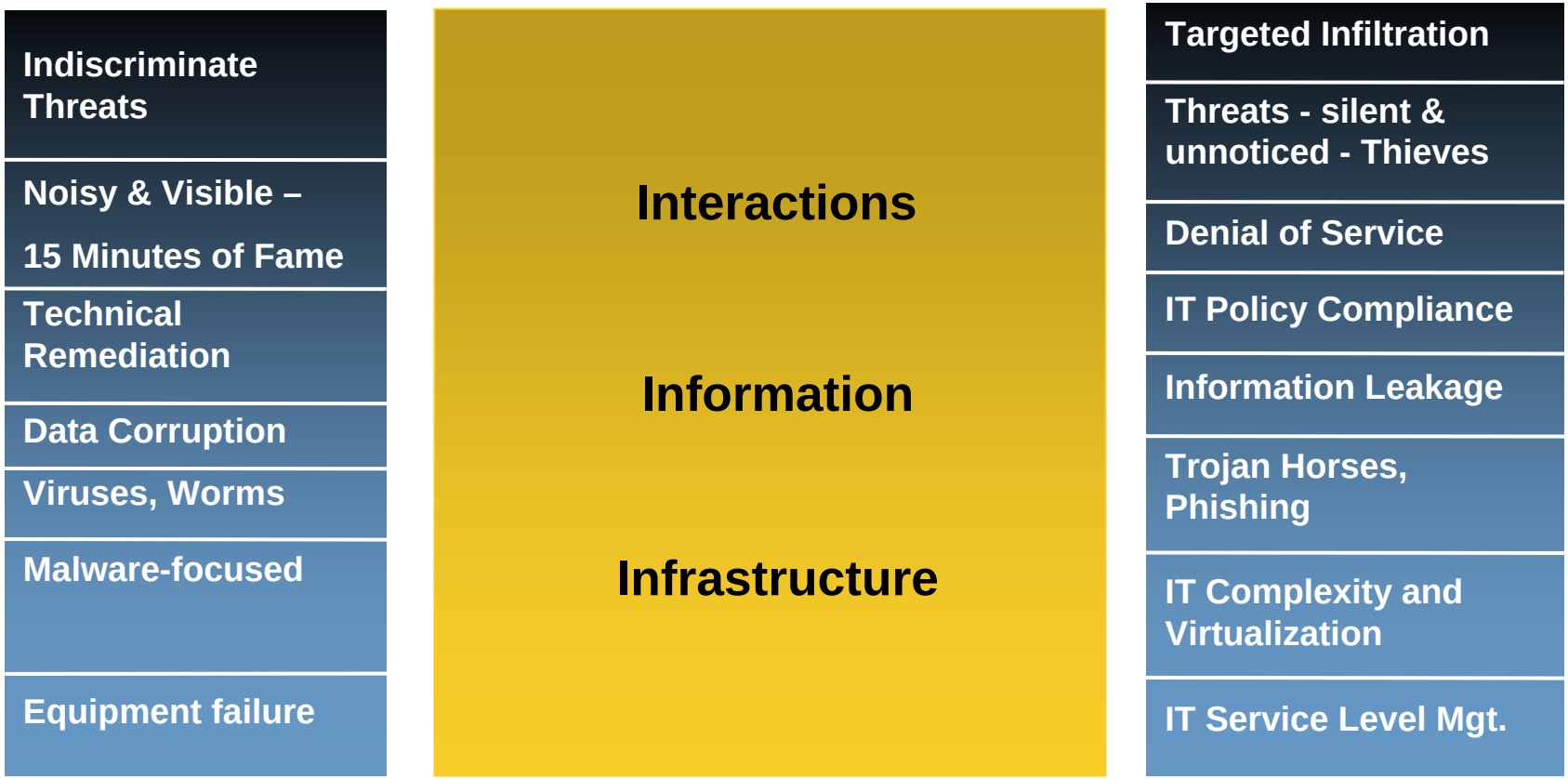
Every vulnerability has its own unique shape. And only network packets with a *complementary shape* can successfully attack the vulnerability.

Once we know a vulnerability's shape, we can create a *vulnerability signature* that checks for that complementary shape.

Such a *vulnerability signature* will then block *all* future attacks against the vulnerability, from their inception!

Why? Because for the attack to work it must have the right shape… But if it has the right shape, it must match the signature.

Technology Evolution Has Created New Challenges



symantec™

Thank You!