

Beyond Applied Cryptography: Designing a Secure Application



Session #66



Managing Complexity



CPU data courtesy Intel Corp.

About Cryptography Research

- Solve difficult real-world problems
 - Systems designed by CRI engineers protect
 \$50B annually
 - Industries: Financial, content, pay TV, communications
- Specialties
 - Tamper-resistance, content security, platform security



About Nate

- Designs network security products
 - RealSecure
 - Storage Appliances
 - NAT TCP splicer, layer2 IPSEC, etc.
- Companies: ISS, InfoGard, Decru
- FreeBSD
 - ACPI, Storage

Cryptography in 3 Slides

	L	ITE	R	AE	s	с	RI	[P	тI			
LITERAE CLAVIS	АВ	a	b	с	d	e	f	g	h	i	1	m
		n	0	P	<u>P</u>	<u> </u>	•	100	<u> </u>	<u>x</u>	<u>y</u> _	2
	CD	1	b	с	d	e	f	g	h	i	1	m
		Z	n	0	P	P	r	S	t	v	x	У
	EF	2	Ь	c	d	c	f	g	h	i	1	m
		у	z	n	0	P	q	ř	S	t	v	x
	GH	a	Ь	c	d	e	f	g	h	i	1	m
		x	У	z	n	0	P	ğ	r	5	t	٧
	IL	a	Ь	с	d	c	f	g	h	i	1	m
		v	x	y	z	n	0	P	9	r	S	t
	MN	a	Ь	c	d	c	f	g	h	i	1	m
		t	v	x	y	z	n	ō	P	9	r	5
	O P	2	Ь	c	d	c	f	g	h	i	1	m
		5	t	v	x	y	z	n	0	P	9	r
	QR	a	Ь	с	d	e	f	g	h	i	1	m
		r	5	t	v	x	У	Z	n	0	P	9
	\$ Т	2	Ь	с	d	c	f	g	h	i	1	m
		9	r	s	L	v	x	y	Z	n	0	P
	v x	a	b	С	d	c	ſ	g	h	i	1	m
		P	q	r	S	t	V	x	У	z	n	0
	ΥZ	2	b	С	d	C	f	g	h	i	1	m
		0	P	q	r	5	t	v	x	y	Z	<u>n</u>
	-	-	-		10000	000000	121744	Sec. 14.14				

2. An alphabet clpher of Giovanni Battista della Porta (No. 5)

1. Encryption Is Not Security

• Many systems use encryption

- 802.11b WEP
- DVD CSS
- Failures result of misuse
 - Constant re-keying
 - Poor key management
- Neither fell first to brute force of key

2. Strength Is Not Assurance

• Strength

- Resistance to Known Attacks
- Example: key lengths
- Assurance
 - Likelihood to Fail to Unknown Attacks
 - Example: SSL 3.0 hash/keying

3. Use standards

- Good standards last
 - SSL 3.0 (1996)
 - SHA-1 (1996)
 - DES (1977)
- New crypto suffers 50% mortality rate

• Committee designs



- Obscurity
 - Increases cost for initial attack, but not repeat attacks
 - Reduces relying party's ability to gain assurance



 Fixed certification standards

 Standardized evaluations only catch standardized attacks...

		All second and CAR functions to section of
UCT 8, 1155 biochestra to Call con Blazer	alter Rieland	subtractions for the study from set in
SCDI. 1151 bincheder in Coll and Molec	der Beisend of	
16/09 2151 Biblinks of Genesics		
15 TR 7151 Bassishes of Canadian Laborat		
SCDD 3120 Cv3 Binlard	· · · · · ·	
NUCCE 1111 Cut Bistory Laborations		
Us T.B. 3520 Materials Reform		
VCDI 4520 or 4650 Developmental Boing		
MCCR 4830 or 4660 Developmental Bolon	aboratory -	
THE Realities difference of Elect. Indexe, 10	in land Theory	and a set one set of the second set of the
ACDD DECEMBER (MEMORY & DEC. HOLDE, DV	est toris, o tests	a approved two writing conversals into a
- MC09		
	_ :::	
COD Ancienty Requirements in CAEM, WAT	THE PROPERTY (Sea	page 7 for minercare grade requirements
CHEM 1111 General Chemistry		\ <u></u>
CHEM 1131 General Chemistry E		
CHEM 2311 Organic Cherawryl		
CHEM 3121 Exgenes Chemistry Laboratory		
GHEM 2001 Organic Cheresory 0		
CHEM 3341 Organic Chemicity Liberatory	di	
CHEM 4711 General Stocheragoy I		
MATH 1200 Calcelos and Analytical Cesin	en y le la la la la	
PFIT'S 1110 or 2010 General Physics I		
PH//S 1120 of 2020 General Physics II-		
PMV8_1141 at 2020 General Physics Laboration	retory	
re Curriculum Requirements not Satisfied Requirement Watten Communication (lover division) Watten Contest-	Course #	Comments: AP, Test, Transfer, etc.
And the second distance in the second s		
Gigure and Gender Oversity		
Guiture and Gender Diversity United States Context		
Gature and Gender Oversby United States Context Distribute and the Arts (aver division)		
Culture and Gender Oversity United States Context Liferature and the Arts (over division) Contemporary Societies		
Cuture and Gender Diversity United States Content Literature and the Arts (taries) division Concernsorum Societies Hoads and Values		
Column and Gender Doorsity Dated States Content Unmaken and the Ahr (baren Schlieg- Contemporary Societies Reals and Walves Uterative and Like Ahr (upper Schlieg-		
Column and Gendler Chevesty- Dated States Content Lifershare and the Afric Idaver Skihligen- Contemporary Statestics Tools and Valver Utenable and Usaker Utenable and Usaker Utenable and Usaker Utenable and Usaker Utenable and Usaker Utenable and Usaker		
Galant and Gendre Diversity Diversity and States Content Utersitive and the Arts (down sinhiber) Concersponny Sociality Disch and Yalven Utersitive and the Arts rupper similari- Warten Connectication turper similari Orthog Thering		
Gature and Gender Develop- Dated States Control Extensione and the Afs (tancer Schnitten- Contemporary Societies Useds and Values Useds and Values Useds and Values Useds and Values Used Schitter Schitten- Official Tacking USL Language. Office Series fol Coverse 5	20%e	
Geture and Gender Downsty David Steels Control United Steels Control United Steels Control Contemporary Stockston State Steels and Video United Steels Advisory Stockston Withon Control Steels Official Theory Official Theory Official Theory Official Theory Stockston Control Steels Stephenemet	20ve Courso #	Cananeatis
Geture and Gender Devicely Dated States Control Dated States Control Date States Control Date States Control Date States Control Date States Control Date States Control Date States Control Date States Official Parking Official	20Ye Coutso #	Cannecis
Geture and Gender Downsty David States Control United States Control United States Control Concerptory Statestas Totale and Video United Statestas United Statestas Web and Control Statestas Web Control Statesta United Statestas USL Language, Ellise Kenis not Coverd 4 Stopplements	2074 Courso #	
Ceture and Sender Devicty United States Control Daniel States Control Daniel States Concerptory Stockets Date and Video United States Write Commenciated Wite Control States United States Control Theory States Control Theory States Control Theory States Control Theory States Control Theory States States Theory States Control Theory States States Theory States Control Theory States States Theory States Control Theory States Control Theory States States Control States Control States C	2074 Courso #	Camposit
Geture and Gender Devredy Deleg Stephen Control United Stephen Control United Stephen Statutes Concerptory Statutes Topological Statutes Water and Statutes Statutes Water Commission Larger disk Cont Octical Theory Control Statutes Stephensons	20ve Courso #	Cannoxis
Gebure and Gender Downsty United States Control Literatures and Die Arts United Schlader Concerpsony Statestas Statestas and Vickes Ukenber and Die Arts Upper Schlade- Wirken Communication Lapper Schlade- Wirken Communication Lapper Schlader Wirks Lappage, Chine Kenne not Coward & Stephenement	20ve Courto # String Total Is	Cannexis
Gebure and Gender Devredy United States Control United States Control United States Control United States States States States States States Water Commenciation Lapper Schlade Within Commenciation Lapper Schlade Within Commenciation Lapper Schlade Within Commenciation Lapper Schlade Within Commenciation Children States States States States States States States States States States States States States States States States States States States Upper Division Cracits Revealed National Upper Division Cracits Revealed States States States States States States States States States	Zove Course # Sting Sciells commute	Cannor::s
Gebure and Gender Councily United States Control Literatures and Jac Arts United Schulers Concerpoory Stockets State and States States States and States States Withon Communications Lapper Schuler- Withon Communications Lapper Schuler- Withon Councils Arts States Sequences Councils States Sequences Councils States Sequences Councils Needlan States Councils Millional Opper Division Cracitle Novelands Councils States States Councils Needlan States Councils Needlands	Course # Course # Bring Tetal Is- acroments	Cannoxis
Gebure and Gender Devredy Deleg Steele Control Unterstee and be Ark dever similation Concerptory Stockers Topolo and Video Unterstee and De Ark tapper similation Water Commission tapper similation Orthur Thereity NTS, Language, Other Kenin not Covard A Requirement Course Development Covards Noted Nitrand Upper Division Cracits Notedarful Course J	Borre Courso # Bring Total Is accoments	Cantoriis
Geburg and Gender Devredy Dated Steles Control Literature and Die Arts Upper Schlade- Contemporary Stockets Stable and Wilker Uteraber and Die Arts Upper Schlade- Wirken Communication Lapper Schlade- Wirken Control Die Arts Upper Schlade- Upper Die Arts Schlader Die Schlader Schlader Schlader Die Schlader Die Schlader Schlader Schlader Die Schlader Schlader Schlader Schlader Die Schlader Schlader Schlader Schlader Die Schlader Schlader Schlader Schlader Die Schlader Schlader Schlader Schlader Schlader Die Schlader Schlader Schlader Schlader Schlader Schlader Schlader Sc	Zove Course # Sting Tetal Is accounts	Cannonis

- Requirements that go against security

 More speed, more features, less cost, less development time
- "Hail Mary" security evaluations
 - Too late: Need security by design



Example: Crypto Storage Product



- 1. "We'll encrypt the data."
- 2. Read crypto book
- 3. Argue about algorithm choice
- 4. Argue about key length
- 5. Implement using downloaded code
- 6. Test
 - 1. Encrypted data looks "random"
 - 2. Data decrypts correctly
- 7. Ship!

Failure: Cipher Mode

- Customer generates secret image
- Encrypts it with new product
- Result?





What went wrong?

- Focused on unlikely attacks
 - Algorithm
 - Key Length
- Overlooked likely attacks
 - Improper cipher mode
 - Others: RNG, key management, sidechannel leakage, etc.

Actual Risk vs. Perceived Risk

• Real Quote:

 - "Smart cards with triple DES are three times as secure as those using single DES."

Everybody knows this is wrong...

Attackers almost never waste time and money on brute force

Even when it's easy, there are easier attacks



Protocol Analysis



Simple Protocol Analysis

- On three big pieces of paper...
 - ① Chart the protocol flow
 - Include every message that can be sent
 - Error messages, optional messages, etc.

② List what can be discovered about each cryptographic value

- Each crypto step generally reveals something new
- List everything (helps catch unintended interactions)
- ③ Diagram the state machine of each participant
 - Include negotiated options, failure states, crypto, etc.
- Reconcile possible end states against objectives.

Common Protocol Weak Spots

- Algorithm negotiation
- Version negotiation (backward + forward)
- Man-in-the-middle
- Message replay (within a session, multiple sessions)
- Message forwarding & impersonation
 - A connects to B, who connects to C pretending to be A
- Certificate handling & validation (or lack thereof)
- Out-of-sequence messages
- Error handling reveals information
- Denial of service
- Timing analysis
- Excessive complexity or lack of defined state machine
- Improper or inadequate use of hash functions
- Inefficiencies (round trips)
- Redundant information
- Management/debug functions (code upgrades, etc.)

10 Suggestions

- Goal is higher assurance that system meets security requirements
- Security is absence of functionality
- This is hard...

• View security in economic terms.

Assign a dollar-value to your risk. Get management support for the estimate. Spend before problems get out of control.

View security in economic terms. Think about how risk is allocated. Where are the single points of failure? Will those who control your risk share it? Are the people you trust actually trustworthy? What is their historical track record? Do they make unsubstantiated claims of "security"? Who can vouch for their work?

View security in economic terms.
Think about how risk is allocated.

Be humble and know your limits.

Don't mistake confidence for experience. Encourage people to look for flaws in your work. Don't assume attackers won't "figure it out".

10 Suggestions



 View security in economic terms.
 Think about how risk is allocated.
 Be humble and know your limits.
 Make realistic assumptions. Assume that users are lazy and gullible. Assume that engineers make mistakes. Beware of the rear view mirror. Your greatest risk may not be what went wrong last time.



 View security in economic terms.
 Think about how risk is allocated.
 Be humble and know your limits.
 Make realistic assumptions.
 Minimize complexity. Isolate critical components. Beware of complex interfaces. Have the courage to resist adding features.

Complexity is a <u>security flaw</u>.

- View security in economic terms.
- **2** Think about how risk is allocated.
- Be humble and know your limits.
- Make realistic assumptions.
- Minimize complexity.

O Spend more on evaluation than design.

Evaluations can only prove <u>in</u>security. Make sure evaluators are <u>skilled</u> and <u>objective</u>. Don't impose unreasonable restrictions. Requires creativity, experience, attention to detail.

- View security in economic terms.
- 2 Think about how risk is allocated.
- **B** Be humble and know your limits.
- Make realistic assumptions.
- **6** Minimize complexity.
- **6** Spend more on evaluation than design.

Be a skeptic.

Assume systems are insecure unless you have evidence to the contrary.

Avoid anything undocumented or untestable.

Ask tough questions and demand responses.

Don't be impressed by the line:

"We can't tell you for security reasons."

- View security in economic terms.
- O Think about how risk is allocated.
- **B** Be humble and know your limits.
- Make realistic assumptions.
- **6** Minimize complexity.
- **6** Spend more on evaluation than design.
- Be a skeptic.

O Plan for trouble.

What happens after a breach?

Will you know if there was a breach?

Keep good audit records.

Are "impossible" attacks really impossible?



Image courtesy NTSB.

- View security in economic terms.
- 2 Think about how risk is allocated.
- Be humble and know your limits.
- Make realistic assumptions.
- Minimize complexity.
- **6** Spend more on evaluation than design.
- Be a skeptic.
- 8 Plan for trouble.

⊙ Use both internal & external expertise.

Risks are much higher if you rely only on just one. Get multiple opinions, especially if you fear: piracy, fraud, or espionage.

- View security in economic terms.
- O Think about how risk is allocated.
- **B** Be humble and know your limits.
- Make realistic assumptions.
- Minimize complexity.
- **6** Spend more on evaluation than design.
- Be a skeptic.
- 8 Plan for trouble.
- Use both internal & external expertise.

Study all layers of the system

Transistors up to business objectives

Unsolved Problems

- Why does the future take so long to appear?
- Why is it so incomplete when it does?

Some unsolved problems that really bug me...

Unsolved: Application Filtering

Progression of the firewall

- IP address, port filtering
- Stateful inspection (Latest: IPS)
- Application proxy

Unsolved: Application Filtering

- Protocols are multiplying
- Firewalls stopped evolving at the HTTP layer
 - Everything runs on port 80
 - Protocols change greatly between versions
 - "All or nothing" filtering

Unsolved: Application Filtering

- Proposal: developer tools output protocol specification
 - Client and server software use spec to format messages
 - Firewall uses protocol spec to disallow improper messages

Unsolved: Certification Aging

- Certification specifies testing conditions
 FIPS 140: certificate shows tested configuration
 - Common Criteria: profile lists requirements

Unsolved: Certification Aging

- Problem: No one has that exact configuration and soon the vendor releases a new version
 - Windows NT level 2 cert (but without network)
 - Netscape level 2 cert (but you need a sticker)

Unsolved: Certification Aging

- Proposal: Use a questionnaire
 - Vendors answer standardized questions about their system
 - Customers (along with evaluators) use the answers to identify application-specific questions
 - Vendor publishes the results

Conclusions

When designing or evaluating a secure application remember:

- 1. Encryption is not security
- 2. Strength is not assurance
- 3. Use standards

If in doubt, call an expert...



Contact Information

For more information, or to discuss how Cryptography Research can help with a security problem:

Nate Lawson nate@cryptography.com www.cryptography.com

Questions?

Single Points of Failure

Examples

ROM/E ² /BIOS contents	Hard disk controllers	Data backup & redundancy
Key storage & metadata	Revocation systems	Crypto algorithms
Threat detection systems	Engineering personnel	Drivers
Executable program storage	Compiler correctness	CPU execution correctness
Sandboxes	Non-standboxed code	Security protocols
Input validation routines	Passwords & login procedures	Tamper resistance
Software update procedures	Master keys & passwords	

Trust Boundaries

- Designers should isolate keys & critical components
 - Putting all your eggs in one basket is actually good
 - Risking all your eggs in many baskets is dangerous.
 - Fewer critical components means they can be tested better.
- Most products have poorly-defined boundaries.
 - Are the perimeters (or contents) too complex?
 - Typical Windows PC is too complex to secure internally.
 - What can cross the perimeter?
 - APIs, network protocols, chip I/Fs, control/audit/backup data...
 - Analyze single points of failure (inside & outside) [next]

Tools

- Gathering Information
 - Crypto toolkits (Crypto++, CryptoLib, etc.)
 - Statistical toolkits (custom)
 - Bignum libraries (NTL for Lattice Reduction)
 - Compiler, system analysis tools, debugger, decompiler
 - Network traffic recorder (tcpdump)
- Brute force / disaster recovery
 - FPGA board, CPU farm
 - Password dictionaries
 - Hard drive imaging tools
 - Password recovery tools/services
- Tamper Resistance
 - DPA workstation
 - Oscilloscope
 - X-ray, Probe station, microscopes, e-beam, FIB