Foundations of Security: Videos
CS 361, Spring 2020: Dr. Bill Young

Lect	Mod	Wk	Title
01	1	1	Introduction
02	1	1	Why Security is Hard
03	1	1	Security as Risk Management
04	1	1	Aspects of Security
05	2	2	Policies and Metapolicies
06	2	2	A Policy Example: MLS
07	2	2	MLS Example: Part II
08	2	2	MLS Example: Part III
09	2	2	MLS Example: Part IV
10	2	2	Tranquility and BLP
11	3	3	Access Control Policies
12	3	3	Lattice-Based Security & BLP Metapolicy
13	3	3	Covert Channels I
14	3	3	Covert Channels II
15	3	3	Covert Channels III
16	3	3	Detecting Covert Channels
17	4	4	Non-Interference
18	4	4	Non-Interference II
19	5	4	What is Integrity?
20	5	4	Modeling Integrity
21	5	4	Modeling Integrity II
22	5	4	Biba's Other Policies
23	6	5	Lipner's Model
24	6	5	The Clark-Wilson Model
25	6	5	The Chinese Wall Policy
26	6	5	Role-Based Access Control
27	6	5	Storing the ACM

Lect	**Mod**	**Wk**	**Title**
28	7	6	Information Theory
29	7	6	Information Content
30	7	6	Exploring Encodings
31	7	6	Languages and Encodings
32	7	6	Entropy
33	7	6	Entropy II
34	8	7	Fundamental Theorems
35	8	7	Entropy of English
36	8	7	Entropy Odds and Ends
37	9	7	Cryptography
38	9	7	Cryptography II
39	9	7	Properties of Ciphers
40	10	8	Substitution Ciphers
41	10	8	Using Information
42	10	8	A Perfect Cipher
43	10	8	Transposition Ciphers
44	10	8	Symmetric vs. Asymmetric Encryption
45	10	8	Stream and Block Encryption
46	11	9	Advanced Encryption Standard
47	11	9	Modes of Usage
48	11	9	Public Key Encryption
49	11	9	Public Key Encryption II
50	11	9	Cryptographic Hash Functions
51	11	9	Key Exchange
52	11	9	Diffie-Hellman Key Exchange

Lect	Mod	Wk	Title
53	12	10	Digital Signatures
54	12	10	Certificates
55	12	10	Certificates II
56	13	10	Cryptographic Protocols
57	13	10	Cryptographic Protocols II
58	13	10	Cryptographic Protocols Abstractly
59	14	11	Attacks on Cryptographic Protocols
60	14	11	The Needham-Schroeder Protocol
61	14	11	Attacks on Needham-Schroeder
62	14	11	The Otway-Rees Protocol
63	14	11	Protocol Verification
64	14	11	The BAN Logic
65	14	11	The BAN Logic: Needham-Schroeder
66	15	12	PGP
67	15	12	PGP Services
68	15	12	PGP Services II
69	15	12	PGP Key Management
70	15	12	PGP Key Management II
71	16	13	Availability
72	16	13	Availability II
73	16	13	Intrusion Detection
74	16	13	Anatomy of an Attack: CodeRed
75	16	13	CodeRedII
76	17	14	Certification
77	17	14	The Common Criteria
78	17	14	Protection Profile Example
79	17	14	Security Target Example
80	17	14	CC Evaluations