ONFUSION: Obscuring relat pher & plain text. Making s is is hard: E(M1+M2)≠E(M1)+E(M2) FFUSION: Soread the infli are not passed in the URL, not recorded in the browsing history do not reyeal the user/passivd if int cepted (altho allow new passivd if Internet Control Message Protoco y the IP layer to send error me o the source boot replicate same tens resources; can be desured tens resources; can be desured to some differences; — VRUS: Spreads secretly, makes a los of effort to dvoid detection; Needs a loss of effort to infect, is, not a stand-alon TARR FUNDAMORPHE PROPERTY A central key serve to everyone: trusted server Γ knows all scheme that a unique secret key (K_A, K_B) . \rightarrow Problems with $\{DN, Y: W$ with whom he's contacted tacker could capture $\{K_{AB}\}_{K_a}$ message δ . 2) $T \rightarrow A$: $\{N_A, K_{AB}, B, \{K_A\}\}$ owser cooke to be stolen

ALIFOGISTNEOUSY scripts from a origin
website; cannot access/set properties of
documents from other origin/websites.
Same Origin Definition: I) same protocol
(i.e., http or https) 2) same hostname software that appears to be de-but in fact performs malicious The second of th user to meet serint code into webpages iewed by others & stead cookies, into I) REFLECTED XSS AH: website not made the there were the control of J PERSISTANT XSS AH; website is mod-ed, allacker posts script on vulnerable ed, allacker posts script on vulnerable The second to cick on if for similar to the control of the second to the control of the control | Does (IN THE MATHEMATICAL PROPERTY OF THE PR lor A; (when it seekes to A vis MAC addit 1998)

1980

1980

1981

1981

1982

1983

1984

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985

1985 Virus length is limited as if ca overwrite tool much of IROS INSERT!

Fore causing robot scan for against a first of the IROS INSERT!

Final DETECTION: scan for against a struction's found in Rnown viruses.

Signatures should be long enough that legitimate code is not mistaker identified to be infected (talse prive). Signatures that are too long ke to scanners missing variants of virus. AND armonics from the some context of the source of the so being the law of the l **MOULAR ARTHMETIC; same as n cept some positive int n che that final result is (mod n)-ed in modulus not prime, then so won (n + n) modulus is (n + n), then so won (n + n) modulus is (n + n), then (n + n) modulus is (n + n), then (n + n) modulus is (n + n), and (n + n) modulus is (n + n). The sum of (n + n) is (n + n) mod (n + n) in (n + n) mod (n + n). It came (n + n) mod (n + n) is (n + n) mod (n + n). It came (n + n) mod (n + n) is (n + n) mod (n + n). payload from which a signature is ge-repied. Verig uses a simple encryption repied. Verig uses a simple encryption when virus proposals to a new file? a when virus proposals to a new file? a decryption engine decrypts the peat of decryption engine decrypts the peat of personal contact, for it is short reported to the peat of the side to defect the virus body will be decrypted as an the virus body will be decrypted as the virus body will be decrypted as the peat of the peat of the peat of the side to defect the virus body which we do not side to defect the virus body because the them, A final three countries residently and the countries residently to the countries residently to the countries residently to the countries residently to the countries of th well SCT vector vocates and the total particle state of the particle state of the particle state particle state of the particle state of the particle state of the particle state of the victim state of the particle stat acker could input carriage return & list feed to spool separating HTTP respon header & body: like reflected XSS, we user to excellent the control of the By adds. If SNs guesses the system of the control of the percy as the victim of the control of t wessure of cript injected into wessure by the how CSF took plysons attack works: XSS attack, starts by barsing current page them finds whatever seed tolken is on a state of the state of t gmining to a solution but is nature to their presence?

**METAROPHIC View DETECTION:

**METAROPHIC View DETECTION:

**METAROPHIC View DETECTION:

**ETAROPHIC View DETECTION:

**COUNTY OF THE VIEW OF THE VIE were hope in dependent ergrey to mental limit once teams or attacker, injectory or and the limit of the limit — BEFORE assisted FOR Best Attack: incree boots; multiple 15.1 such cases incree boots; multiple 15.1 such cases in source adverse; Victim allocates resources for each request until source sources for each request until source adverse; Victim allocates resources for each request until source adverse; Victim allocates resources for each request unit pour connections. Eventually, the half-open connections. Eventually, the half-open connections requests are accepted, leading to demial requests are accepted, leading to demial excepted, and the proposed of the control of the So the sequence of the sequenc DES: Data Encryption Standard
AES: Advanced Encryption Standard
AES: Advan change via neural most and recyr auth to public crypted with the spublic population hash; the neural recipient can decrypt using sender spublic is sender could have encrypted the text we received viding suthentication in on-repustation. The control of the co or each user; solve problem via 13:74:30 [13:11114] Designate a central centity Provider to handle auth (describes with portion of the key (subkey Kn) Coulty (Har-FESILL-1900M) the implication of the nice in the property of "The Additive Rue: Authorities my same than the thing with each modified my same than the regard the next modified my same than the regard the next modified my same than the regard to the the same than the same t makes are given to agile in days. The second of the second (q) where q is address in allocated Attacker can set values in their hunk tag so that free will set free werwrife a memory location cho-Series who from a support material we common the series who shall be supported by the series of the series which is not series when the series social solverined by the perce. It is considered correctly of the considered con with a support of the property sprintf@pll – Similar to a swifth sta henl – Each code entry invoes the lut tion pointer in the GOT – ic. sprintfl pll may invoke imp GOTIkl where k the index of sprintfl in the GOT – if if we change the pointers in the offs table we can make the program call o own code, i.e., with objedning 20 — STEPS: b4 auth can be don must register with auth server. I provides ≥1 URIs (Uniform Re identifier) where tokens should b luser (resource owner) receives The state of the s PHER BLOCK CHANNOS: Make every block dependant on ciphertext of prev block (at EE.B. mode). For first block, use initial (IV). IV doesn't have to be secret but never be resselles-EB. Block which is not been considered by the control of the contro text friessage.

EFFNCE against REORDERING atk: use N + nonce + Sequence num to misgs. If m come out of order, or a sequence nu ber is missing. B can detect that tamping has occurred; This also preventifrom dropping messages; need to imment sequence num if itash. – A ser "Symposium of popular Delegation and the delegation of the appropriate property of the popular delegation of the popular d replay-define & MDC = H(M | seq n SSI GISUINSSOCKI SI NYSSI en/de-cu packets by sending between endp-lese ver-client/browser) thru not thr routers so that transitory routers ac read/alter packet data: client CAN be ed, but does not have to be; has 2 phas — A) Key exchange/handshalke: does at Fig this with accent opers as pre case over the accesses where the MoMSES correct is tage input gin or a maller outful [18,0]—it is meritage, it hash-value, [11]. Insay compression function.

**DEFILE SHORM MESS provide integrity suth-soon expudiation of the provide integrity is guith.

**DEFILE SHORM MESS provide integrity suth-soon expudiation of the provide integrity is guith and the provide integrity is guith.

**DEFILE SHORM MESS provide integrity suth-soon expudiation of the provide integrity is guith in the provide integrity in the provide integrity in the provide integrity is guite in the provide integrity in the same head value computing that considerably heads to the same head value computing the provide integrity in the provi Also seeks of between senter or re-sets sector by multiple energible (and tissed for ympletic energible (and tissed for ympletic energible eighters eight side supports, and wh eversion of the protocol is being used. Securely establishes a shared secret the can be used as a session key 3) Au each others identifies, by certification— 1). Clear (C-S) Heljo: client indical which SM; versions & capbers it is can cription & decryption is unit of test than a tunion a fine (i.e. conjuert block ciphers into stream phers). CFB/OFB have security, error & recovery. The present ciphers of the conjuert block that the conjuert ciphers of the conjuert ciphers of the cipher ciphers of plaintext lows performing cipher, operation in advances of the conjuert ciphers of the ciphers of th lisertionry write acces to 0

BLP does NOT provide INTEGRITY policy: be low security level subject can modify and does NOT propose MILEMENT Product, and MILEMENT Product, and of RID-prevents town amongstry data. Interpretable to the product of the pro Security: Stream ciphers have similar prop to the disagreous to tuse same keystream to en-crypt 2 messages to the pad in OTP except pass participants. Similar to the pad in OTP except pass (Reystream) is pseudor-random & generated from much shorter key, stream of random bits is ther used in place of the one lime pad & XOR ed with points support ir see, but intermedia fouters do not; encrypts/authentica the packet payload (Similar to SSL, SS 27 Tunnel mode; for when endpoints not support IPSec, but endpoints ways do: encrypts/authenticates backet header & payload & encar layer that the integrity level of a. t. — "Did on scoop 24" (42) 2(3) (2) — "Did on scoop 24" (42) 2(3) (3) — "Did on scoop 24" (42) 2(3) (3) — "Did on scoop 24" (42) 2(3) (3) — "Did on scoop 24" (42) 2(3) — "Did on scoop 24" (42) — "Di Keystream depends on plante sists of a shift register. Every c ated is shifted into the shift reg as input into g. Ciphertext has k is secret key. Receiver can use the that the MAC matches the message, thu source of the message as well as the con set in some content of the content o -BE-HAC (MAC using symmutor cryption to block representations of cryption to block representations and the same as block cipher; need to hash may BEFORE encrypting, using the same statement of the s mary or intelligence or with a control as the contr BALALA-CBC-WAC

BALALA-CBC-WAC

WHY CBC-MAC NEO DIFF MAC & ENCRYPT KEYS: If the lion key is compromised, having a separate MAC key had the title integrity of the data is not affected. Similar the integrity of the data is not affected. Similar the least the recompromise! same device: IPSec often doesn't inter-operate well (poorly standardized im-bementations), so both sides of the con-hection are required to have the same vendor's devices = 5) If a specific service is required & aumonted by SSL, is better to select SSL. $\frac{1}{M} \frac{1}{K} = 0 \text{ to the constraint of the gas an effective constraint of the interpreted sight, and constraint of the interpreted sight of the sight of the constraint of the interpreted sight of the sight$ sagress must be obessed s) injected of the control 1) IP-see has lower overhead because many users can use the same sectire establishment for each channel.

2) IP-see supports pre-shared keys so PKI is not needed.

3) If access to an entire network greguired VPN software/device using aller stipport of mactime to use say mitigantly weaker encryption schemes or shorter currents on the say that the say th Freedal Desponent: Incoval is normally the an extended an extended and page tautis, uncompared to the party to the injected code via ending apostrophe e.g.
'; update C set name='attack';-need comment - to indicate end of injected

