I when the state of the state o Very term infratery that infratery Privary Pri sym K= (M, K-Gad) VKiK Vmin: d(e(m, K)) 411= x gym K-1 Ke Kejis Gad) Hispickolle (m, p) is in Makerdarus is three single in Voter substitute (45°) exist frages Miniahariniarang Recoursen manget way, beside (water ele, w) = alway, w) = ir(wate) [851 — food g gras wellishing of the board that the transfer of the contract ki neve Technifen, Truining Das Pensing, Gericht. Cursur-ele, with etwan, -wa) = 91(10,1) [PSA Failule Watchile Ruhestern prinzip (; strin; mun (ki mod m) Weste 14e & Zopen; duber 15t(e, p(n))=1 thome c-recombinishing the string of the production of t Security tehatz gopen of the hoperifer "nucle mech cleaning the expense of the parties of the pa Known Try We abhitish white retz sell61-13 ho= fleenc(xo,xy)) hi=f(uei(hi-1,xi)) suche g & Zp mit endly)=9 Choosen Mess. Statisharine (Make (1° o, d)) past 1/4 and 4 for many to the many sound of the many Adaptive cheoren M description of the state of the Zide-Existential Fergy selective Univerial total break Aprobabilitistisch =7 semantiget gicher Totp Time-based Ventizieren ingress condition with increation confidence in 24 finder manifect of elater, i), w) 4x; qualishely and Diffie Hellingen (benerierung) stranding = loted up/total (up-down) = Alt Watte + All P) Strange Chipton eight and Sei Prim p, b= Zp Generatory EAp

Showing the continue of the control of 41= H(m) in medy Zajallovariable Thebronzeit Pathefunttion & Angrafer modell north Polev Nac / Logium 5= 1=9 (H(m)+ +x) morty V= 94 = 642 malp may Fin-Pitsh Schlysselaustausch aktiver, passiver Expressibles Made U: P(T>5+1 T>5)-PCTZD Transport/ Generier way Mitf: 5" R(1) dt & Meedham - Schroeder T GCTRK(11B, xg11-11xn)=1,-1, Wie schlinel Parallet For (7)= it For (1) Res (1): 1-th (1-For (1)) Expansion B decret thuring H=e(O,k) Library: Timestamp ENA, NB3 KYA. Peder schlingel-55H varigate recessary strategies entockels Witchely rebeat , Puritybility, (14,11)-Hemming Lade by 16-bip Karrigeran shureholder strong = 2.0,

shureholder strong = 7

vict yenindung ENB3KPB tolorune: Redundanzon, sefety Sheekpointing specitions Zunted and Indianal hat made became this 25617

Physikuliach, zeitlich Zusutzieformationen - Vorzögert Rieustruktur - Performance akanten and besont ties 25617 (t,n) schwellwest Kryptosystem migh. Atteck Enteriore gleiche It. auch Seftware-bedustungen mit stich firenthams
Statisch ta-1 Systems standby - feliererkensung coporaterlich -Performence - Kontin - Synchronisation min the emolich beheim + Verfügber trusted Deder, lembiner, Konmunikations kunik Azureision überzeuren dutich to 1 syrum money Roll (1) Res) (1-Ru) (1-Ru) The sym kaypt begenüber Buls Awasgeben Shamive Secret sharing farketage ton 9+1 x tot Listing - B bestariff WEN in 18 Polynom in 2p plrim (10) = k [Len (Al) (4 leal 4) Schlüssel in O(22) statt O(2") Ast-Guanten-Kryptographie =>K-länge verdeppeln Zero-Knowledge Beneine Grovers Algorithmus durchsucht unsortierte Datenhank in OHA) Sharen {5,52,-3, 3= {(afig), (m, f(m)),-3+Perfekt Short Algenthmus zur Fakterisierung zufühlig asm it giftan) + 1 = 7 get (an) bruphen (2016) Tilsenerphinnes 6HASH THE CIPBUH) Rekentruktion Algorithmus von Peytsch f: {217-1413 Quanten finile q'=1 moden Pwaint a f (0,13 und Permutation p Simons Algorithmus Of f(0)=f(1) a ungerader 95 += 0 =7 ron vorne P Plint v V mitt be to 19 Challange Problem zur Konstantheit Fund normaler dem ar-1=km = bin Fermell = 7 99 T (q = 1 1 m) = 1 + Verfahren wieder no read down Ansitze für gugatensisher Wahl in Zubleapiere (private) Committe Reveul-Verfahren 0:= {pii falls a 3 b= 11 Integrinit van Daten Code-bused cryptographic MAC-Mandatory Access Courrel R= Freuel, 14 me Code-bused cryptographic eleven husha (public) is ignieren versifie attichen BAC più fulls u: 16=0

Maltinariate " plansport - (Diffie) - Einmyt signitume fulnum 1.12. uns Paux Role R. Zollen ausschlass + Unternehmensatrythus waf Regel 129: 5 5 C: 5+0256 Erweitert M gt signification to 12 aus Paux Role & Rollen ausschlass + Unternehmensstruttur auf Regel pegis 56: 5+022 Erweitert M - Leine Meditioning Covert of Control of the Change of the Country particle ordings in a mile class Assessment of the Change of the Land of the Change of the Change of the Change of the Country particle ordings in a mile class of the Change o benutzerbestimmet statemmeise All keine formen stat dynamisch in sestion separation of Multilevel security partielle Ordnung in miterchan Supersingular elliphed Authoritistan Rechte für zinzeine O Zeilen (L. Richererseiten srift) partieble Ordnung dury etwichte Label L (that gead) (b) 4 (l) 4) strong Tranquility

Rechte für zinzeine O Zeilen (L. Richererseite Rep (P) Riskjer Richererseite Label L (that gead) (b) 4) & (l) 4) strong Tranquility

Misk O+3(R) Unix tren - bestägene strong Rep (P) Riskjer Richeren (1445) (les and Laufzeit Andergag and Les and Laufzeit Andergag and L curre isogenies Antinge General Referenz R- Eread White, exel, 100 mg of for R- Eread White, exel, 100 mg 1. Definition. Workship states of Single-Sign-On 540 Suberheitsnihllimin Objekt Ficherheitsklussen Speur/Dynamite-Phishing: zielgerichtef Mar Rechte aktires Roblen Kontaupinupin Web Security Trend online Banking; beld vor sicherheit Benitz (Smart Card Cookse) zentrole Authentigierung für Doma he Leuter Modelle i Abstraktion 3. Meibanismen (hyplomen) Taken Principal User (tient chaptops, smartphones, Drittparteren,-) server jewanerd Estimestumps Ke, C, Na, T65 statisch - direkt Authentifizierung: Sniffing Mishing, specifing, x 54, ltickjecking, sersion riding Identifie + (Menge Attribute) - Dietostable 2.8. Side-Channe (Lient (EKGTGS 1 1/3)Ke, ETGT3 KTGS Authenticator A= (CAP, timestamp) Mittle Das Rebinding, sersion Hijacking Authorisierang 12.0. Perse) - engl- nuthenticution Kusius (Ac), Kas (TGT), S, N2 7 T65-Ticket Grenting Server Ki=h(Poss) Server (Apache, Ngint, 1811 Websphere,) Autentifikation/-fizierung (Prüfugng) Merkmale Attacky Buffer Overflow, Pirectery Traversel, Weak Puss words FAR-Falsch positiv Kustig (KGS, N2), Kg (TGS) T Autorisierung Eintliment, Verifikation DBMS landere Dienste (Salmy Sal, Onackle PB, Claud, Sterage Pru.) einseitig/wechselseitig Universalitet History Merkingle Wissen 2 B. Rassworter KyslAil, Ks (tys) timestamp Eindeufigkeit cifetime, Kc,5) - Weak Passnords Gendtkining land Bestanding Kest EER Equal Error Rub Schutz HTTPS CA-Zertifilate Kc,5 (timestamp Vertray Lich Keit queiches bei meureren servern (Lientseitig (Web-Browser) Erfussparkeit Stouminest, Hautfarbe SOP same Origin Policy - unsichere abertragung schwerer

A MK & benner | DF Hosin Performance/=>peicherung Referenziaten Angriffe Offline Cracking (collinestamp) Schulseffingre Keylogger tors tross orgin Resource Sharing Akzeptunz Overlass the Hosh 1 the Ticket Forschungssicherhait Lerofile Makhing Betweets pringre "Eve key Derivation Funktion CAP Content Security Policy Colden Tickes Leigenes Tet mit Kr65) A Was wenn Eve Finger nicht geheim => Lebenstert Terreracting i Web-Frame Sicherheit, Web Tracking, Wa kie Gerning Gibrerticken leigenes I mit Kg) Busich: Konnekter Doctype Spanherung Minutien Bsp Schwachstelle Annendunyan) private Browsing Konzepte: In kognito Mody US H==h(K) Reihbswtable 7 Buffer Overflow Metacluty V\$ H' == h(K, Sultio) Erkennung serkennen bakannte Fragmente breken Aues Control fehlender bounds check von Noteer Inputs -Window of rulner bility - einfoche Anderung Variablen oder stack-Frame micht mehr erkamt Rücksprungadresse CHAP Challenge-Response Kein Inline (77 reaktiv-statische Signatuven - viel überschreibt folgende Voten auf Life Stack Design-proper Authentification, weak-Passwords RAD - Brauss Kkennen 79 am Enile Variablen oder stack-Frame mit Impli : breken Impl. Lack of audithing uniacity RAND) - Mitm beneit my Proultivi schlie Bende Tags Sandboning teure Entwicklung Beispiele: resticul Priviledge Est glution Crass-Browner Kompa-Stack-Smashing aberschreiben mit Adr. secrettunction Malware (Malicious software) Henristiken Performance PHP-Hypertext tibility parameter-based-access control (bei Lehler Abstyrz) Preprozessor Masnahmen: ASLR Adress Proce Layout Rambonisation Trejaner-Programm mit unerwünst blem Neben effekt Insecule direct object Reference Stack lungries: Prinfwortauf stack gof Programme beenifung Würmer selbständige Ver preitung übers Internet exponentiell bis alle anfälligen SQL-mjektions Non-executable-stack : nicht gegen stack-smashing unzureichendgeprüfte Weitergübe von Nutzerdaken un Poten bunk Kunsom ware Verschlisseln Outen verlangen Lösegeldemichere Operationen Vermeiden begen making timen Leine Nultiple studements, least privile apec Verbindung oderdrehen mit Veröffentlichung x55-Cross Site scripting Viren : einfügen in Wirtspregram in 2.8.35 Web-Anwendung interpretiest Clientseiby gehendene Parometer Astant = Smy syli aprepare ("" 3 Physen Typen: executable infectors Theader | virus | Gide & Outo persistent: spenberung auf Webserver SQL: and Eer or, 4 comment une relation Insertion encrypted Viruses Peciphering | Encrypted Code | key 14mt + bind-param ("5" 4 string) auf selbem (Got) umonal select...
(2.8. Teil URL) reflected direkte tusgabe, Ausführung Astmt + executely "in fint Estennang Februs auf 3 Replication polymorphe Viren begin nasmen - schwerig Veranderung bei Replication z.b. againstauter integ Junkcode Placklisten, aber riele agairplente Verhindert statische Erkennung durch Viventwelkils automatisiert Schüdliche Zeichen

THE DELIGIT - LEGISTANDE AND ASSESSED ASSESSED AND ASSESSED ASSESSED AND ASSESSED ASSESSEDADAS ASSESSED ASSESSED ASSESSED ASSESSED ASSESSED ASSESSED ASSESSED ASSESSED ASSESSED ASSESS

	10 - ALEN 10000 CHOST Oland for makes my En 10 16 Kind . Allen Still Cottonal
051 Modell Open Systems Interconnection) Firewalls Linux 189tles A	upon Detection / Prevention by them 105/1195 of may resident Application: 55th Vertain lich keit Treplay protection upon Detection / Prevention by them 105/1195 of may resident Application: 55th Vertain lich keit Treplay protection upon Detection (Integritation of the protection of
Delton & Dhug. & Thatile - Duris Umale Prints / Malanagle I have well Tomas pour	Llower Netzwerk, Hostebene Annihittsmuster transport TLS (layer sec.) Integritati (pertet forward con.) - CHNA)
Lucion and 14 Llink 249tomdolog statische Ligh	e an kecker " at the Korrelighton Everyniedown (chent Helle, 5 DUE 85 A At 2728.60.11 244 256
with the toler south and the straightful to	borbook below Try Mary Pay 1614 Amount lives with a Vall Whe Hellming DHE-POK THEY HAY THE
MATIMUM AND ANDER CONTROL OF MOTORING TO MY MANTEN	Controlle Metalleal hongo ren chilingho Delan
TO UM TO DIE BUT WAS I WILL TO SHOWVALUE TO THE TOTAL OF THE TOTAL OF THE PROPERTY OF THE	1 WILLIAM 17 1 1 2 M
Mai specting en dunchleiten nach MAC Breaklagt hachste niedrighte fran	The state of the s
MAI specifing einfach much MAL Breadcast hachste m. Train thosts chizoschon 2 -3 Train 11-Aufleiung 11-Aufleiung	The souler witerfreng prome on on continuous with the
" rent regimente mit IP Internet P.M & who has (IP) Browless	WIN addances Notalinas Notalina
romen shire Pakete Protokou) ura gre tell comip)	THE FOR THE - ZWISLINE II COURTE VERYS IN THE BOTT OF THE FOR THE FOR THE FOR THE PROPERTY OF
Network Layer Merzen ARP specting 24stunteles => 50 milen	Remote towers and to ste controlled wansperancy a softentiane ways with the part of the Frances
LALINE FOLLOW STATE STATE OF THE PARTY OF TH	Rechwer im virtuellen Netz Seit boogle, Iran, Digitatur Handl Soft fail Web of Trust 2.B., PGP für Emuils ed Wiederuf: Zertifikats speirlisten (CRL) in Zert revlinkt Keyserver, verwendung
1. 14 10 La	hen notokel DOT Online Zertifikat Status Protokell Stattaernen Trend nur wonn von Meta-Introducer right
Checksumme DHIP OLLS- DUE NEGGET	Partly followed by the total the solution of the the total the solution of the total the solution of the total the solution of
regment nummer Portnummer 125 5MTP, 80HTTP DHCPS peofing Fre Autwor	
Flynkontrolle 143 IMAP. 443HITPS Line Switch DHIP non 11	
Flyskontrolle - B. 143 MAP, 443HITPS Lo gyng Switch PHLP nor 11 UDP, TLS Bradbreste noch Empfonger 1 5000 Con von Metal	Marketeilum in duto nome systeme BEP Hijacking Ziel innorhalb des Admins Problem Wiez Reclirection (off mit anderen Ambiffs- vektored
user Peroperte col/ ransmission control Protoco of Pour Control 28	Announce monts aktualler Routen Sub-prefix Sub-version (MITA) (schwer zu zrban)
Destil al Same Das Variable	
Presentate Invite mehrliche Rechner	A South of the state of the sta
Duly niver 150 100 DD05 Vistributed Dos Botnetz	reat some Firem RIPE
2 B ACIN A LEW A PROPERTY OF PROPERTY	eretyrn 11 / 12 R Internet Kouling do BEP-Speaker 2000 1 2 100 00V1
Kompeliate reason in the property will brachte	eserver deway hinterlegung Prefix Weinste Zu teilung 124
Serialisterung TCP syn, Syn-Ack Acks (Verschlüsselung) son-Floud: Verbindungen bleiben offen	RPK1 2022 Ca. 50 8/Adresse Knapphel strigeral
Funktionen für Software Sen-Ack Algeture Stoofen MA Amplification to	RIOTO 1 PUDUICUTION POINT = = Kepositores
2. H. HTTI, PTI, SMTP UDP FLOOD unerworketes UDP - ILAPP-Error ds.	Mot wort 1 ROA Route Origin Authorization - knot against 16- Proces
Ethernes IP/TCP Applicates Data Data Data	RP Relying Party Received Received about and Month Councils xoul
heuder h. H. H. Dung	Reposition PRPP & Rowallo non 937% other 45 ensteller ROX85
D16	Publicution 7
DNG Application	Point 159nc 166 PSec gegen Suprersion of musico 3 Backup 204 für origin 451 5K1-subjekt Key Identifier (refers to RPKI)
PILEST DIVINITY INVENTE : INVOIT	Portakel 451+457 Prefix, & 451,641, 492 3, 69/16129
50A-start of authority	402 Personanh 452 4 453 Prefix & 451, 9K11, 452, 5K12, 453*3, 4516 12, 516 233
Automises in Gerver/Regolver, 5 tub Kegalva	* signed over but not industed in the forward BGPSEC update
UDP parts Top für große Mibrichten	
Mulmichanter caded 4/	PMS lach Poisoning
Heister Metadatan Forwarder	historisch Kasbourella 1997 -> Bailiviele Revel
Flag awas Kon	hur cachen von 5, Le
This represent ~ 2 octov 6140	Residven was Off Ryth hur cachenvin Subdomain vents
Anzahl Records in Sethimen	Residven was Off Rath
Trunsaction 10	
Question Syktion	1 2008 14 14 14 14 14 14 14 14 14 14 14 14 14
2.8. INNUNE rangle arg. INA 5	exw"
Anonor section	Nit Mit Mit Mit All Part + suber stub Res = rek
RR set zu anfinge	org. Dott für Henrife Reminer
won example org. 42 1N A 93	ant stub Renolver in puttic Wifi copy Zulangson Fattisung
Authority bektion	b Ma
Ns server	Beginfluggan VIITY Bal Notes Lillen
23. jexapple-org. 3600 10 1/9 ns example-org	
	W/S Tumpling
Auditional sektion.	- oft antificie
2, B. 1P 24 ng Es,	- Langsum +2.3- Expitation
	of the Att Chipperson
Weitere Angriffu	Vernaltungsantwand: (Post) SPF
Pomuin Hijacking	PKIM, Permin Validation, DANE
Flooding Angriff gergen Dus server	
Zenour destills	