با عرض سلام خدوت تمامي دوستان
اين دفعه با توجه به بحث طولاني كه در رابطه با نحوه پاك كردن پسورد بايوس يا عبور از پسورد بايوس بود تصميم گرفتم تا اونجايي كه ميتونم مقاله ايي جامع و كامل در اين مورد ارائه بدم و كليه راه هاي سخت افزاري و نرم افزاري در اين مورد رو براتون شرح بدم:

ابتدا به سراغ راه هاي سخت افزاري ميرم:

1- برداشتن باتري مادربورد:
در اين روش شما ميباست باتري نگهدارنده اطلاعات بايوس رو برداريد و مدتي صبر كنين سپس باتري را در جاي خودش قرار بدين.كه البته اين مدتي كه بايد صبر كنيد براي مادربورد هاي مختلف متفاوته ولي اكثرا خدود 10 الي 15 دقيقه هستن. يه راه ديگه هم هست من روي مادربوردهاي گيگا تست كردم جواب داده :در اين روش ديگه صبر نكنين وقتي كه باتري رو برداشتين يه بار دستگاه رو روشن كنين وقتي سيستم عاملتون بالا اومد ShutDownكنين،بعد اقدام به نصب مجدد باتري بكنيد.(البته در اين روش همه چيزي كه مربوط به زمان باشه به هم ميريزه،مثلا اگه برنامه رجيستر نشده ايي داشته باشين ممكنه ارور بده).

2- استفاده از جامپر ها:
در اين روش شما ابتدا يك جامپر رو جدا ميكنين سپس دوباره اين جامپر رو سر جاي اولش قرار ميدين توجه بفرماييد كه در طول كار دستگاهتون بايد خاموش باشه.البته بعضا در بعضي از مادربوردها ديده ميشه كه با برداشتن اين جامپر دستگاه خود به خود روشن ميشه در اين حالت شما خودتون بايد اقدام به خاموش كردن سيستمتون بكنين.
اما مكان اين جامپر كجاست؟
جا هاي مختلفي ميتونه باشه چون توي مادربوردهاي مختلف متفاوته ممكنه:در امتداد لبه مادربورد باشه يا نزديك باتري مادر بورد(CMOS) باشه يا نزديك پردازنده باشه ، بعضي از توليد كنندگان مادربورد هم ممكنه بروي اين جامپر برچسب هايي با اين عناوين:

dipswitch CLEAR - CLEAR CMOS - CLR - CLRPWD - PASSWD - PASSWORD - PWD

نصب كنن.اما بهترين راه اينه كه شما به دفترچه مادربوردتون يه سر بزنين و محل دقيقشو بيابين اگر هم بلد نيستين يا اين كه به دفتر چه مادربوردتون دسترسي نداريد به يك شركت كامپيوتري مراجعه كنين و يا دستگاهتون رو پيش يه آدم متخصص ببرين.

3- اتصال كوتاه بين پين هاي بايوس(اين روش به دليل خطرناك بودن براتون پيشنهاد نميكنم):
از اين روش ميشه زماني استفاده كرد كه شما دقيقا بدونين كدام يك از سيمهاي خارج شده از بايوس وظيفه تخليه اطلاعات رو داره ، براي اين روش هم بايد كامپيوترتون بايد خاموش باشه.

4- عوض كردن چيپ بايوس :
اگه اين راه ها براتون عملي نشد مجبوريد كه يك بايوس جديد بخريد و اون بايوس رمز دار رو با بايوس جديد عوض كنيد،كه البته اين كار شما نيست شما مجبوريد كه مادربوردتون رو بفرستيد نمايندگي تا اونها براتون اين كار رو انجام بدن.
****

راه هاي نرم افزاري:
البته اين روش هاي نرم افزاري زماني به درد ميخوردن كه شما رمز بايوستون رو ميدونين ولي ميخواين كه رمز بايوستون رو پاك كنين يا به هر دليل ديگه ايي

1- استفاده از نرم افزارهاي مربوط به اين كار

2- اگه برنامه ايي به دست نياورديد يا اين كه به آن دسترسي نداريد،از اين روش استفاده كنين:

از برنامه debugاستفاده كنين :
من يه سرچي كردم اين دستور ها رو بدست آوردم،اين دستورات رو در صفحه تايپ كنين و بعدش برنامه رو

ببندين:

0 70,2e
0 71,ff
0 70.2f
0 71,ff

اينا دستورهايي بودن كه من توي سرچم پيدا كردم،اين دستورها حتما بايد توي محيط داس نوشته بشن مثل Commend Prompt

اين دستور ها رو هم دوست خوبمون Soltan-fearيا همون سلطان ترس ارائه دادن:

ابتدا تايپ ميكنيم de bug و اينتر ميكنيم
سپس وارد ميكنيم 70 20 o
و دوباره وارد ميكنيم 71 21 o
آنگاه حرف Q را تايپ ميكنيم و اينتر ميكنيم
حتما در محيط داس نوشته شود و پس از اتمام كار Restart كنيد و وارد Bios شويد آنگاه متوجه ميشويد پاسورد پاك شده است.

با اين دستورها به احتمال خيلي زياد بايد پسورد بايوستون پاك بشه

3- استفاده از شاه كليد ها:

اين شاه كليد ها از طرف توليد كنندگان مادربوردها ارائه ميشه و به Backdoor Passworsdيعني پسورهاي پنهان نيز معروف هستن:

در اينجا چند تا از اين شاه كليد ها رو براتون ليست ميكنم:

Award BIOS backdoor passwords:

ZAAADA	KDD	BIOSTAR	ALFAROME
ZBAAACA	Lkwpeter	CONCAT	ALLy
ZJAAADC	LKWPETER	CONDO	aLLy
01322222	PINT	Condo	aLLY
589589	pint	d8on	ALLY
589721	SER	djonet	aPAf
595595	SKY_FOX	HLT	_award
598598	SYXZ	J64	AWARD_SW
	syxz	J256	AWARD?SW
	shift + syxz	J262	AWARD SW
	TTPTHA	j332	AWARD PW
		j322	AWKWARD

awkward

AMI BIOS Backdoor Passwords:

HEWITT RAND	PASSWORD	BIOS	AMI
CONDO	LKWPETER	AMI_SW	AMI?SW

Phoenix BIOS Backdoor Passwords:

BIOS	CMOS	PHOENIX	phoenix

Misc. Common Passwords

biosstar	biostar	BIOSTAR	ALFAROME
lkwpeter	LKWPETER	cmos	CMOS
Wodj	Syxz	SETUP	setup

Other BIOS Passwords by Manufacturer

Password	**Manufacturer**
merlin	VOBIS & IBM
Dell	Dell
Biostar	Biostar
Compaq	Compaq
xo11nE	Enox
central	Epox
Posterie	Freetech
iwill	IWill
spooml	Jetway
bell9	Packard Bell
QDI	QDI
SKY_FOX	Siemens

BIGO	TMC
Toshiba	Toshiba

البته ممكنه يه سوالي براتون پيش بياد كه اصلا اين دستور ها(نه اين شاه كليدها،دستورهاي پاك كردن پسورد منظورمه) چي رو ميرسونن؟

اگه همچين سوالي براتون پيش اومد من يك مقاله انگليسي كامل و تخصصي در مورد اين نوع دستور ها در قالب PDFپيدا كرده ام ولي چون زياد بود هنوز ترجمش نكردم،حالا هر كدوم از دوستان كه خواست بگه تا براش بفرستم.

موفق باشيد

امير حسين محمودزاده

Tell Me:
Amir.p30@gmail.com
http://arteach.parsblogs.com
http://forum.p30world.com